Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Wednesday, June 7, 2006
Clift
Rita and Ava Rooms
495 Geary Street
San Francisco, CA 94102

AFTERNOON SESSION

MR. BEALES: What's next on the agenda is Subcommittee reports, to complete Subcommittee reports. And I guess we can start with the Framework Subcommittee from Jim, Joanne?

MS. McNABB: Yes. Jim, Joanne, and John.

SUBCOMMITTEE REPORT: FRAMEWORK

MR. HARPER: Very briefly we'll report on some of our activities and plans. We, as all of you know well at the last meeting, I believe, we approved the Framework Document with the assistance of many people's input. And we have been gratified with the extent that many Subcommittees have used the Framework or the ideas in the Framework to advance their work. And we've been comfortable with -- in cases when Subcommittees didn't find the Framework useful. So I think it's where we meant it to be as far as -- as far as the document for the Committee.

And we've been delighted to learn that other people outside of the Committee, even outside the country, our memories fail currently but Australia or New Zealand, a jurisdiction out there has indicated to the Privacy Office that they thought the Framework Document was a useful thing for their purposes. So that's -- we really take pride in that and thank all of you Committee Members for your work with us on that document.

MS. McNABB: Alberta.

MR. HARPER: Alberta. That's in Canada. The Data Protection Commissioner there apparently likes it as well, so that's all very gratifying.

We continue to work on a project that we began thinking about and working on very early on in the tenure of the Committee, a thing that our former Chairman Paul Rosenzweig was very interested in that we -- that we agree is an important topic of discussion and effort. And that's the idea of driving privacy considerations very early in the procurement process. To do that, one of the first steps we've had to take is to try to learn how the procurement process works. And we're not sure if it does.

Evidently in a large, newly-created organization like DHS there are a lot of different things that happen to get mat,riel chosen and technologies selected and programs underway. So our effort to rationalize a component of that process is made difficult by the fact that there isn't a clear structure for getting that done. But we continue to inquire and hopefully we'll have better information about those processes in the near future.

I guess the final item is the work we've discussed also in the past and that continues to generate with the ISPAB Committee, and I'll ask John Sabo to say a few words about that now.

MR. SABO: Thanks, Jim.

As you know, the NIST has an Information, Security, Privacy Advisory Board. The board is actually meeting Thursday-Friday of this week and they have formed a subcommittee as we have in terms of our Framework Subcommittee to take a look at the practices and changes in technology that have occurred in the last decade or two and determine whether or not the implications inherent in those -- in the laws and policies and rules established by the federal government need to be updated and/or adjusted to account for changes in technology.

For example, looking at the application of technology against the privacy principles embodied in the Privacy Act is one example. It's not exclusively focused on the Privacy Act. And by doing that examination, expose the gaps in the ability to implement privacy given today's systems, you know, distributed networks and data collection, et cetera; and also look at new vulnerabilities that might impact your ability to manage your privacy allegations.

So they have formed a subcommittee. They are going to be working with our Subcommittee. And one of the things we will be working out at the meeting this week later in Washington at their meeting and then a subsequent subcommittee interaction will be how best to proceed with this project. I think one goal will be a white paper that will explore some of the issues I've talked about and possibly recommend a set of best practices that you could apply to managing some of these issues.

MR. BEALES: All right. Thank you very much.

I guess next we'll turn to the Screening Subcommittee. And, Ramon Barquin, you are going to give the report.

SUBCOMMITTEE REPORT: SCREENING

MR. BARQUIN: I want to give the report by default, as I was the last one out the door from our Subcommittee meeting.

The Subcommittee had agreed on a process where we were going to review five specific screening systems as part of the initial tentative inventory that the Privacy Office had done screening systems throughout the Department. We did do that yesterday.

The rationale for this was to try and see if we could obtain some insights that would then allow the Subcommittee to start providing broader recommendations that would apply to all screening systems for the department and elevate them to the Secretary through the Privacy Office.

We looked at Einstein. And E-i-n-s-t-e-i-n does not stand for anything. It actually is just named for Einstein. Einstein is a system that is intended to try to consolidate and identify across the whole government, not just Homeland Security, primarily anomalous activity on the networks. This is supposed to be an OMB responsibility, but as wound up sitting in the hands of the Department now under US-CERT.

We also looked at HME, which is Hazardous Material Endorsement. It's a TSA system that basically enables truck drivers to receive, no endorsement, allowing them to truck around hazardous materials.

APIS, also TSA, this is the Aviation Passenger Information System. We looked at SEVIS, that's the Student and Exchange Visitor Information System, which I believe is an ICE -- it's a CBP system. And, lastly, we also looked at the Global Enrollment System which is run by TSA and which is attempting to try and bring together all of the different trusted travel secure, you know, traveler type of information.

We did I think learn a lot from these reviews, which are based on the PIAs, primarily, of these systems. And as we move ahead in the future we will -- that hopefully be elevating some broader recommendations.

There's a lot of work to do, and without it going to the head of the Framework Subcommittee but, yes, we moved your Framework piece, at least I did, in some of these reviews; as well as some of the previous recommendations that we had already put together for Secure Flight.

Let me just end on the note that this is a committee sadly in need of additional resources. As we look at the other brethren committees around here, I count that there are

seven in Emerging Technologies, I believe there are six in Framework, there are five in Data Sharing and Usage, and there are now only three little piggies in the Screening Subcommittee.

So on that note of too much work and too few people, I will end.

MR. BEALES: Thank you. I think the message is loud and clear. And we will try to send in the cavalry.

David, the Data Sharing and Usage Subcommittee.

SUBCOMMITTEE REPORT: DATA SHARING AND USAGE

MR. DAVID HOFFMAN: Thank you, Howard. And I'm just hoping the cavalry don't include any horses or pigs from the Subcommittee for Data Sharing and Usage.

The Data Sharing and Usage Subcommittee has been working on two separate items that we discussed at our last meeting. And we have found, as we progressed the work, that they are quite connected, which I will describe, and I will describe what we were doing on them.

The first piece of work is continuing the work that we have done on DHS' use of commercial data. As many of you may be aware, we did publish a paper on the use of commercial data to reduce false positives. And that document is on the website, and we continue to be interested in any feedback that anyone in the public has on that document.

We are now expanding that piece of work to be a more comprehensive document, which we are entitling "A Draft Annotated Outline on Public Agencies and Their Use of Commercial Data." And we -- the approach there is to get a much better idea of what are the types of commercial data that public agencies have an interest in using and what should be the privacy restrictions on the collection and the processing of that information.

The second piece of work, which we found out is quite related, is to take a look at the Privacy Impact Assessment Process that the Department is using and that the Privacy Office specifically is using, and to provide any feedback that we can on improvements within that process.

So what we have found is while working on both of those that the -- some of the preliminary conclusions that we have come to that we are testing now on the use of commercial data rely greatly on the Privacy Impact Assessment and the processes in the Privacy Impact Assessment for analyzing specific programs. So we are now working on both of these projects together, in parallel and trying to make progress.

I'd like to specifically thank the staff for being incredibly helpful to us in getting information and working with us, specifically Becky Richards and Toby Levin for working with us.

On the Commercial Data Outline, some of the issues that we are facing and trying to understand better are specifically understanding the different models by which the Department or government agencies might access that information and the implications of the different models. By that I mean specifically pinging the data when the database exists outside of the government and just getting a result from that ping, versus bringing the data specifically within the government and what the implications of that would be.

And another second distinction would be ad hoc access to commercial data versus a systematic approach or a specific program, a programmatic approach to accessing the commercial data.

What we have found is that the implications for both systems-of-record notices and potentially the obligation to fill out a Privacy Impact Assessment can potentially change depending upon where -- what model is being used in a particular situation.

I want to call out the Privacy Office's leadership in this area, actually. Maureen Cooney mentioned earlier this morning some of her testimony that she's been doing. And, specifically, I want to call out her testimony from April 4th of 2006, where she called out some of the fantastic leadership that they're showing when she said, "Although the E-Government Act allows exceptions from the PIA requirement for National Security Systems, DHS is implementing Section 222 of the Homeland Security Act to require that all DHS systems including National Security Systems must undergo a PIA if they contain personal information."

The Committee would like to commend the Privacy Office for taking this position. We are building that policy into our document that we're working, and analyzing what the implications of that will be. At the outset, we -- some things are a little bit unclear and we're going to continue to work with staff and try to gather more data on this. Specifically we do think that it's a fantastic thing to take on that obligation.

We have some concern and it's unclear whether the Privacy Office actually has adequate staffing and resources to be able to accomplish adequate reviews of all of those Privacy Impact Assessments with the current resources that they have.

We also have some concern with the review of the Privacy Impact Assessments. It's unclear to us exactly how much authority the Privacy Office has been given by statute and within the Department to actually review those Privacy Impact Assessments and mandate the changes to be made in specific programs. We think that's a very important thing that needs to be taken a look at, and some clarity needs to be defined upon that and brought out.

And the last thing that we're somewhat uncertain about is along with the authority, I think along -- goes with that, it's unclear exactly how much autonomy the privacy office has, how much they can act as an autonomous body versus having to depend upon

relationships with the other groups within the Department. And we're going to seek more information on that and understand it.

So the next steps on this document that we have had as a draft within the subcommittee and a couple of the other members of the Committee have graciously agreed to provide us some feedback on it, is to go out and seek some information about specific programs within DHS that would -- either are collecting commercial data or are pinging commercial data, and to get an understanding of either how they are doing it or how they would like to do it, and then apply some of the principles that we have been working on to see how they would actually work in practice. That's all.

MR. BEALES: All right. Thank you very much, David.

Questions, comments, anything else from the Committee?

If not then we can move to our first panel. We actually have I think a pair of panels this afternoon on some topics that are really central to a lot of what we do on this Committee and that I personally am really looking forward to.

Our first panel will be on exceptions of privacy in public spaces, both real and cyber. And I think what we'd like to do is to introduce each one of our speakers, ask you to speak for 15 minutes, and then once all three speakers have had a chance to talk, then there will be a half an hour or so for the Committee to ask questions. And I would ask Lisa Sotto to please introduce the panelists.

MS. SOTTO: I would be delighted.

MR. BEALES: Oh, the panel should come up. I'm sorry.

MS. SOTTO: Please be seated. Thank you.

PANEL - EXPECTATIONS OF PRIVACY IN PUBLIC PLACES

MS. NICOLE WONG, GOOGLE, INC.
MS. DEIRDRE MULLIGAN, UNIVERSITY OF CALIFORNIA AT BERKELEY
MS. LILLIE CONEY, ELECTRONIC PRIVACY INFORMATION CENTER

MS. SOTTO: Thank you very much for joining us. I will introduce each one of you before you speak. I think you're each designated for about 15 minutes apiece.

Our first speaker this afternoon is Nicole Wong. Ms. Wong is the Associate General Counsel for Products and Intellectual Property at Google. She's a frequent speaker and author on issues relating to law and technology. And I know Ms. Wong has been thinking hard about data-retention issues these days.

We'd love to hear from you. Thank you for joining us.

MS. WONG: Thank you very much. I'd like to thank the Committee for the opportunity to speak on this important issue of privacy in public spaces. I have to say it, and I think I mentioned it to a few people during the break, we don't have much to say on the issues of physical camera surveillance that have been largely discussed today.

Having said that, however, at this moment in our history the Worldwide Web is perhaps the biggest public space we have. It is a virtual space where people can gush about their favorite bands, share their family vacation videos, or their thoughts on religion, the environment, or our world's leaders.

And as the Supreme Court in the landmark case of ACLU versus Reno found, the content on the internet is as diverse as human thought. And as such it fulfills a critical democratic function.

So in the short time we have today I thought I would take a moment to talk about the framework in which we think about privacy at our company and to answer any questions that you might have.

At Google we develop our products around our users in terms of usefulness, look and feel, and indeed in terms of privacy. User trust, including the trust that we will keep personal information secure, is something that we work to earn because we believe that's one of the things that brings our users back to us again. We cannot succeed without it. Whether it involves our Web Search, Blogger, or some of our newer services like Google Page Creator and Google Spreadsheets, these are important issues for us to meaning.

When we talk about our approach to privacy a bit more, at Google privacy is really not just an interest for the company's lawyers. It's an issue for everyone, from our engineers to our executives. And for that reason we think about user privacy in the very design of our products. The privacy policy that accompanies those products hopefully is just an explanation of how users can use the product features that protect their privacy.

Our touchstones in this area are transparency and choice for the user. Transparency about what information is collected and how it is used. And choice as to whether a user provides such information to us and how we will use it if they do.

There are a number of examples of how we actually build that into our products. Google Toolbar, for example, is a downloadable application that let's you search the Web from the toolbar. It has a great pop-up blocker. It can even check your spelling and other neat bells and whistles. In order to provide that service, the Toolbar sends the URLs that the user surfs and some other information back to Google. And although we don't require any registration information or personally-identifying information to download and use the Toolbar, we think users should know how it works before they download.

So before you can download and install this program, we display a warning page that says in large, bold letters: "Read this." It's not the usual yada- yada. And then we tell them what we do. That's transparency.

Another example is our Personalized Search Feature. When you sign up for a Google account we have a feature that let's you track the searches that you've done in the past and use those searches to improve your search results. This is particularly useful if you forget a search that you did last week, which I often do. So in a very clean interface we display the search history associated with your Google account.

The really key feature of this service, however, is how we built choice into the service. The user can edit and delete any search or click stored in personalized search. In fact because sometimes you may share a computer with someone else and want to search without recording your searches, for example, I don't want my husband to know where I searched for his father's day present, we added a pause button. It's like a snooze button on your alarm clock, and the service won't record searches or personalize them until you resume. That's choice.

We do recognize that these services require a careful balancing to deliver the best possible product with appropriate consideration for user privacy. And some services, particularly personalized services, can't be offered without asking for this P2 data. This is particularly true of products which I'll describe as communication or community products, like Blogger or Google Groups, Orchid, or our Google Page Creator, products that make up the Web's public spaces, if you will.

We offer these services and require only a minimal amount of registration information, but by their nature these services tend to include personal information from the user. Importantly then, we offer the user control over that information, allow them to decide what to include in the Blog, the Group, or the User Profile Page. And this control includes the ability to terminate an account for such services as the user wishes to withdraw from the public space, if you will.

Our goal in offering all of these products is to give users as much information, as much transparency as possible so that they can make informed decisions, and also offer the appropriate features to control their personal information when they use our products.

Let me turn to some of the challenges that we see ahead. The privacy challenges are growing as we move rapidly to Web 2.0, where computing is a service model with all of the user's important applications and data running and live online. This includes services that we have today, such as Webmail, whether it's Hotmail or Yahoo Mail or Gmail. It includes online file or document search, like Yahoo Briefcase, Microsoft Foldershare, AOL Xdrive.

There are calendars. There are invitation systems, and blogs. And, increasingly, the supplies to rich media storage, like photos, videos, and music that are being held on third-party servers.

This new model allows you to log onto any computer, cell phone, or any internet-connected device and have all your applications and data instantly accessible and searchable. It dramatically expands the amount of data that a single user can store electronically. And we think this next evolutionary step for the Web will be tremendously valuable to users.

That said this model also brings serious challenges to ensure that privacy is protected when users choose to move their data from their own PC to a server-based service. Whether you keep a journal in your bed stand drawer, on your home computer, or on an online service like Blogger, Live Journal, or Diaryland, your entries ought to have the same level of privacy protection.

As a starting point, Google supports and believes in baseline legislation for consumer privacy in the United States. But recent press stories and, frankly, our users tell us that individuals are increasingly concerned about how the government accesses their online information. And with regard to electronic data, the protections are simply not the same.

It is not the case, for instance, that data on your PC is protected equally when it is maintained on a service-provider's computer. For example, in the U.S. data on users' PC in their home is highly protected by the Fourth Amendment, requiring probable cause and a search warrant to obtain it. The same data held on a server by a corporation, on the other hand, may receive less protection under the Electronic Communications Privacy Act, which for some types of data imposes a lower standard for government or law enforcement access. Indeed, in some cases as little as a subpoena.

The recent proposals from the attorney general and congressional leaders for a data-retention law raises the stakes since Web 2.0 services will dramatically increase the data on third-party servers. There are many issues raised by data retention, but among the most important is how will we balance legitimate law enforcement needs for information, whether it's for identifying child pornographers or terrorists with innocent users' privacy interests? Who will have oversight? What are the burdens of proof and who bears them?

I recognize that Google's decision to resist a DOJ subpoena earlier this year is in a different context than what we're discussing today. It was a civil case. The data requested was not tied to personally-identifying information, such as registration or IP address information. But we were as surprised as anyone that we were the only ones of 34 companies that received a subpoena in that case to challenge that subpoena.

Without that challenge there was no apparent oversight on what was an incredibly broad and untargeted request for data, including users' searches. In the parlance of this Committee's framework, who will decide whether there was an appropriate and defined purpose in the Web 2.0 world and its data requests? Who will decide whether the principles of minimization have been abided by, that the data quality is sufficient?

In the Web 2.0 world, how can we ensure that there is protection at that process level for our users? We think these issues require serious discussion among industry, law enforcement, and the public. We are pleased to see it begin here because, again, for us this is about user trust. It's the touchstone for our business and for our values.

Thank you very much.

MS. SOTTO: Thank you very much, Ms. Wong. That was very helpful.

Why don't we -- we'll reserve questions until we've had a chance to hear from each of you.

Deirdre Mulligan is our next speaker this afternoon. Ms. Mulligan is the Director of the Samuelson Law Technology and Public Policy Clinic at U.C. Berkeley School of Law. She is an attorney and a leading advocate for free speech and individual privacy rights on the internet. And Ms. Mulligan has served on a National Academy of Sciences committee to examine the privacy implications of authentication and identification technologies.

Thank you for joining us.

MS. MULLIGAN: It's a pleasure to be back before the Committee talk about another incredibly important issue, where technology is advancing at a rate that far outstrips our legal framework. And I feel incredibly fortunate that this Committee was pulled together by DHS, and really applaud you for the work that you've been doing. It's been incredibly thoughtful and I think quite important. And I hope that you'll play a similar role here.

I actually reframed my talk. Instead of talking about Privacy Expectations in Public Places I retitled it, "In Defense of Public Spaces." And I want to start by talking not about privacy but by talking about the places that are increasingly become subjects of visual surveillance. These are the National Mall, the town square, the public centers. They're the place that Habermas called the "public sphere."

They're critical components of our democracy. They're the places where we have those chance encounters. They're the places where the body politic is supposed to run into the ideas and the people that it might choose not to associate with.

It is, in fact, the melting pot and it is the place where democracy is supposed to spring forth. These are incredibly important, vibrant places. And I think it's important to think about these as not fungible, replaceable, places on a map but as part of our politick,

part of our, I guess I would say, constitutional geography. And I think it's important to think about the implications of wiring these places not because of the physical -- their physical geography but because of the activities that we expect them to be able to support. And we've protected these places for a whole -- against a whole host of changes, so as the mall replaced the downtown public square or the company town replaced the downtown, we've continued to expect those places to be able to support and defend people's ability to express themselves and to get up on the soapbox and to leaflet and to organize and to protest.

And it's important as we think about changing the architecture of those spaces that we appreciate the reasons that those spaces are what they are and why we decided they're important to our democracy.

The second point I wanted to make is that we are very much at what I like to call a constitutional moment. And fortunately, as is quite typical, we end up at a constitutional moment with respect to technology without lots of constitutional guidance. And when I say we lack constitutional guidance I mean specifically that we don't have caselaw that's on point from the Supreme Court.

The Court hasn't been faced with the question of when you wire every single town square, as they've done in Great Britain, do we have some Fourth Amendment violation when those cameras are targeted 24/7 at the bulk of the population, which is not suspected of doing anything wrong. The Court hasn't been squarely faced with that question.

Some of the courts have been faced with questions about surveillance and they've decidedly said: Well, actually, no we're not yet at the point where constant visual surveillance is on the horizon and we're going to actually set that question aside.

Despite the fact that we lack constitutional direction from the courts, I would ask the Committee to think and reflect upon what the Constitution means at a slightly larger sense. I was asked to talk about privacy in public places. Often that means the Fourth Amendment. The Fourth Amendment certainly protects privacy, but it actually doesn't speak of privacy. Right, the Fourth Amendment, the Constitution are important because of the ways in which they seek to structure and order the relationship between citizens and the government. The Constitution is about limited government. It's about limiting the intrusion of the government into our lives.

Our private lives can occur in public places. The Constitution recognizes that, even if the case law does not always adequately do so. And I think it's important when we think about visual surveillance of public places of the scale that we're envisioning that we realize that what we're seeing, and which Dr. Norris has pointed to, is the potential to greatly shift a power balance.

The watchers become invisible. The watchers become remote. The watchers become all-seeing. And the population becomes in many ways completely incapable of knowing what, when, where, and for what purpose they're being overseen. And an environment like that I think we know breeds distrust.

There was a question asked about whether or not we have any empirical data about whether or not constant surveillance actually alters people's behaviors, and I think we don't have a lot of information about public spaces. It's really hard to get that kind of research through the Committee for the protection of human subjects on campuses, but I think we can look at other cultures that have been far more oppressive.

We can look at China today. We can look at Stalin's Russia. There's a wonderful quote from a law review article in 1974 written by then Associate Justice Scalia where he said, you know, in Stalin's Russia there was very efficient law enforcement, there was very little privacy, and the winds of freedom did not blow.

And so I think, you know, we can look historically. There are many environments where the presence of the police and their surveillance, it may not have been just visual surveillance, in fact they were using the eyes and the ears of the population as their surveillance technique, rather than mechanicalized, but we know that those societies were far more repressive. They were far less encouraging of the democracy and dissent, and those things do go together, that we experience here in this country.

The third thing I want to say is that today I think the most troubling element of where we are is how we're getting there. In the 2004 budget, it's my understanding that DHS devoted $193 million to the acquisition of cameras. This is through grants that are being given out to localities.

Those localities are not engaging in any form of public process that's apparent to me. There's no question either, I think, about the purpose to which these cameras are being deployed, whether or not they're the best use of resources, and very, very little attention paid to the potential effects on civil liberties, civil rights, or the free movement of people in which those -- in areas that are going to be surveilled.

And so I would say one of the most troubling things is that if we are, in fact, going to become a place where instead of us being able to ask Dr. Norris, "Where are the cameras," he says, "Well, I can't even tell you where they're not," right. And I think we have a question about whether or not we're going to get to a point where we can't tell people where there aren't cameras because they are everywhere without any public dialogue about whether or not that's someplace we ought to be.

And so while the Court may not have told us what the Constitution requires, I think that we owe it to ourselves as a society to ask ourselves what the Constitution demands. And I think that is what we need for a free and open society. And, at the very

least, that means we need some modicum of public debate and discussion about whether or not every single small town or large city in this country should be under 24-hour surveillance by the government.

So I have three, I think, one modest and the other two are perhaps a little less modest recommendations. The first is one that I think this Committee can act upon quite easily. The Department of Homeland Security for its own procurement of technologies, as every other federal agency, needs to consider the privacy effect of the technologies that it chooses. And it's required to engage in a process called a Privacy Impact Assessment, which I think at this point in your tenure you know far more about than I do.

And I would respectfully request that you make sure that they apply that to the grants and the research that they support. They are at this point, I believe, the major funding source for the camera projects that are being established across the country. And it seems that it would be quite simple to require local communities that are going to use DHS money to procure technology that has an impact on privacy, which I would say surveillance technologies we probably uniformly agree does, that they too go through a Privacy Impact Assessment.

The second is less modest but I think perhaps more important. My students and I recently worked at the Constitution Project and a document, which you'll find outside, for guidelines on public -- Permanent Public Video Surveillance Systems. And a large section of that document is devoted to calling for a civil liberties assessment.

And so the request is that this process of installing cameras becomes one of public discourse and debate. It includes a cost-benefit analysis. I think it would be quite disappointing to know that enormous sums of our taxpayer dollars are going towards the procurement of technology that has very little effect in disrupting criminal activity and, on the backhand, ends up being misused. And there are many examples of misuse, which I do go into in my written testimony.

And I think this could look much like a notice-and-comment period. My hope would be that it would have real opportunities for public consultation and public input, but I think that we need to have a public conversation about the deployment of these cameras. It shouldn't be something that's done in secret with guidance only from the local police department.

The third is that we truly do need to have a national debate. I think there is something wrong when there is $193 million flowing out across the country to purchase video surveillance cameras and Congress has had two hearings since 2002 about whether or not visual surveillance in public places is appropriate. And so we need desperately to update our surveillance laws. This is true of our electronic surveillance laws. It's even more true of our visual surveillance laws.

To the extent that we think about vision and we think about hearing, that they're sense. And we're moving into a technological edge where we're going to be able to enhance all of our senses. Our sense of smell, our sense of sight, what we can hear, our ability to taste and touch are all going to be enhanced by technology. And it's quite interesting. You know, clearly the Supreme Court has found that despite the fact that you're in a public place, you do have some expectations of privacy with respect to the secrets that you're sharing, right.

This was in the context of a phone booth, but the Court very clearly said that privacy protects people, not places. And Congress reacted and not only do you have privacy over that wire line, but you have a privacy expectations in your cordless phone communication, even when it was not encrypted. You have a privacy expectation against the government using a hyperbolic mic, right, enhancing their sense of hearing even though you're speaking in a public place. And so I don't think that the conversation about whether or not we have privacy with respect to visual surveillance has to end with the fact that we're in public. People often talk about Eskimos having, you know, a hundred ways to talk about snow, and we have one. I think perhaps we need a hundred ways to talk about public.

Sometimes when I want anonymity I'm really happy to be going, you know, to some foreign city and I get off and no one knows me. Clearly I'm in public, but I feel really private because nobody knows who I am. And I think we need to have a much richer dialogue and to think a little bit more clearly about what kinds of privacy expectations people need to have in public places, not for the individual so much as for the relationship between individuals and their government. And I'm going to end there.

MS. SOTTO: Thank you very much. I know we're going to have a lot of questions for you.

Our next speaker is Ms. Lillie Coney. Ms. Coney is the Associate Director with the Electronic Privacy Information Center, otherwise known as EPIC. She focuses on nanotechnology, surveillance, civil rights, and privacy, and a whole host of other areas.

Thank you for joining us.

MS. CONEY: Thank you for having me. I would like to thank the Committee for inviting EPIC to offer comment at today's meeting. EPIC, as you know, is a Public Interest Research Center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC takes public positions only on matters of concern to consumers and as an advocate for civil liberty and privacy protection.

I'm pleased to participate in this panel's discussion on Expectation of Privacy in Public Spaces.

Privacy is difficult to define in the abstract, but much easier for individuals to describe in their own context. All too often this definition is limited to only viewing privacy as the state or condition of being free from being observed or disturbed by others.

There are three prescribed states of privacy: Solitude, small-group intimacy, and anonymity. The subject of our panel discussion, Privacy in Public Spaces, falls under the heading of anonymity. Anonymity can be found when a person is in a public place or engaged in public activity. Anonymity in public spaces means that an individual or group of individuals can still anticipate and benefit from the freedom of not being identified or falling under scrutiny.

Anonymity may seem counterintuitive. How could someone expect privacy yet be in a public place, such as walking along a sidewalk, sitting in a park, joining a demonstration, or attending an entertainment event.

People in public places are aware that they can be seen and they, in turn, can see others. But the key to understanding anonymity is the inability of human beings to recall in great detail their own past. How does anonymity exist? It exists because people are not engineered to remember but are designed to forget.

Significant events can become part of long- term memory, but short-term memory is a processing plant that functions with little regard for order or accuracy of events, places, people, or things.

In our modern digital communication age we are awash in information. We have the potential to take in more data with the assistance of technology than any generation of people to proceed us. Our minds exist in a hurricane of information, which reinforces the anonymity of privacy in public spaces as a real part of societal expectations of protection from unwanted intrusion or attention.

Under the condition of anonymity individuals found in public spaces can find privacy because they become part of the situational landscape. Unless the person is of sufficient notoriety or a celebrity or a public figure, they can and do experience the privacy provided by anonymity. Therefore, people can and do expect privacy while in very public places as long as they are conducting themselves in a way that is not seen as extraordinary.

The definition of "extraordinary" does vary based on custom, culture, and social norms. For example, it would be -- it would probably take a significant event such as what occurred on September 11, 2001 to imprint long-term memories on the mind of the typical New Yorker walking along an uptown sidewalk.

I make three key points in my written testimony about the broad public adoption of CCTV technology for surveillance purposes. First, the use of surveillance cameras raises far-reaching constitutional questions to implicate the right of citizens and, most significantly, people who engage in peaceful public activities while in public spaces.

Second, the benefits of video surveillance systems as a means to reduce crime and deter terrorism have been significantly overstated. Studies from London, England and Sydney, Australia make clear that the value of cameras is overstated and that money is better spent on officers than on cameras. Moreover, the particular effort to promote the use of face- recognition technology may be one of the biggest corporate boondoggles in recent history, costing taxpayers hundreds of millions of dollars with little benefit to show in return.

It is also reported -- it is also important to note that this technology can lend itself to racial profiling.

Third, that's systems are being interposed in public settings without the benefit of uniform guidelines that equally balance privacy and security. Some efforts at rulemaking in this regard disregard the important privacy protection of anonymity as if it does not exist. These rules also may take too restrictive a view of the expectations of privacy and First Amendment protected activities. Many of these proposed systems of public surveillance lack adequate means of independent oversight. The reporting requirements are vague. The policy on usage and retention may be insufficient. The definitions are too narrow and the auditing is too limited or nonexistent.

In conclusion, local, state, and federal law enforcement agencies must develop a healthy perspective about print transparency in the use of CCTV systems. They may see transparency as an opportunity to question their behavior or conduct, and may see that as questioning their authority as well as their integrity. However, transparency is a key component of a functioning, healthy democracy. It can be translated into public policy discussions that allow citizens, policymakers, and the media to assure themselves that a local, state, or federal government agency is functioning as intended. In this context the process of providing transparency is referred to as open government.

Open government can be accomplished in a number of ways which include: Meetings like this, public meetings, public rulemakings, notices, reasonable public comment periods, access to rulemaking proceedings, official reports, and open records laws.

It would be important to note that as government agencies are offering funds for surveillance technology, especially of the nature of CCTV, that that information should be made available online. That if a community is applying for those funds, that application should be available online. If the funds are awarded, that information should also be

available online. And they should encourage public comment periods, encourage those local entities to actually engage in an open and broad discussion about the technology. I strongly endorse what Deirdre said in that regard.

The application of CCTV technology by law enforcement or financial security should not exclude -- be excluded from open government objectives. In addition to the method described, the adaptation of CCTV technology may require additional opportunities for public comment and discourse.

It's important to note that since July public surveillance right here in San Francisco have grown from a pilot program of two cameras to eight cameras. Now there are more than 30, and the mayor is requesting funding for a hundred more cameras.

This city has also received $1.2 million in grants to decide how, not whether to install, a downtown driving toll system, looking to London and its thousands of camera with license plate recognition as a model.

And the city's new WIFI system in its RFP proposal, it asks that vendors describe whether those systems that they were providing information onto the city would also allow remote wireless camera connection.

Three things are very important to note about the environment that we're looking at right now. There's not a lot of information on how this technology actually works, what it's long-term or short-term benefits might be or detriments might be. It's hard to measure something retrospectively that's going out in ways and in places that aren't clearly identified.

The research community that will come in after -- even sometimes before the cameras are actually installed to try to measure and monitor and report on and do research on this whole new area of our public space experience will have to figure methodology, so that as we look at comparing studies that will be generated over the long haul, how can we compare and contrast these studies. Are we looking at the same things, are we measuring the same things? Can they be used to make statements about where we are or be able to benchmark and measure as the adoption of the technology comes along? At least help other communities evaluate whether they would like to go down that same road.

That's something else that's very important and rarely have heard discussed is how unique the culture of law enforcement really is. How they view themselves within our society, how they view society as a whole. How they even view decision makers and how they process information is very unique.

It's not just a job. It's a culture. It's a way of life. And because of their role in society, which is very important, it is a tool of society. Law enforcement doesn't provide for or

make sure that we have the liberties and freedoms that we have. The Constitution does that and the laws that flow from that do that.

Their job is to focus on the narrow, very small portion of the population living in a very free and open society who might engage in activities that threaten the life, liberty, and the ability to pursue happiness of others; and bring them before the court to answer for whatever conduct they've been brought before the court to address.

They are bound by the rules and the laws that are written by our society. They know that the exercise of the discretion that they're given as law enforcement officers may require that they answer for that. So they have to document, they have to write, they have to provide transparency to all of the activities that they are engaged in on behalf of the state. That level of transparency provides security to us all.

There is, as I would say, a police state of mind. You don't have to live in a police state to find it, but it is a part of all free societies that have also the tool of law enforcement as a component of that. And I think policymakers and decision makers should be well informed about that aspect of that community and its very, very important service to our broader society.

Model guidance should be developed to assist local, state, and federal agencies in the administration of CCTV systems, which should include strong support of open government procedures -- I cannot overstress that -- that allow access to the decision making and implementation process.

A good start for formulating this guidance to law enforcement and public officials can be found in the American Bar Association's Technology -- Technological Assisted Physical Surveillance Guidance, which EPIC assisted in developing.

There are also the Guidelines which Deirdre mentioned for the "Public Video Surveillance, A Guide to Protecting Communities and Preserving Civil Liberties" developed by The Constitution Project.

I thank the Committee and look forward to receiving your questions. Thank you.

MR. BEALES: Thank you.

Thank you very much to all of our panelists. I think this is a very interesting discussion, and the number of raised flags suggests it's raised a bunch of questions.

Lisa poked me first, if she didn't raise her flag first, so I will give her the first question.

MS. SOTTO: The benefit of sitting next to Howard.

Jim and I had a very interesting and rich discussion at our last meeting about the definition of surveillance. So I would agree that public debate is very necessary. We can't

even agree. Those of us who are reasonably well informed about the issue can't even agree on the most basic thing and that is how is the word "surveillance" really defined, what is it's meaning. So I would wholeheartedly agree. Deirdre, you made reference to Dr. -- or maybe you didn't -- Dr. Norris referenced the DHS study on surveillance cameras. And do you know anything about the study, do you know what is being studied and whether any privacy considerations are involved in the study? That's my first question.

And then second, and you -- the answer may be no. Second is you mentioned that you would like to see an update on surveillance laws. Could you expand a little bit on that? Thank you.

MS. MULLIGAN: Sure. I don't know, I don't think I know anything about the DHS study. And maybe somebody here does? No.

Maybe Dr. Norris can inform us all.

And the second question was updating our laws and what needs to happen. Well, so I think for a whole host of reasons we avoided dealing with visual surveillance. It's a hard question. I avoided working on it for a whole bunch of years, actually, because it's really hard. And so when police walk down the street, clearly we don't expect them to avert their eyes, right. And so in some sense, yeah, you don't have a whole lot of privacy in public in that if there are other people around, they can see you.

So part of the question is thinking about how does technology change our experience of being in a public place. If we think about privacy as being about expectations, how are expectations shaped? Clearly we take cues, right, in shaping our expectations.

So when I tell somebody, well, you don't have any privacy in a public space, what do I really mean? Well, generally I mean there's some mutuality, right. If there are other people there, they see you, you see them. And, right, you might duck behind a bush or you might decide not to pick your nose right now, right. But you also are able to assess whether or not you know any of those people, right.

You may be wrong and it may be that somebody else has a better memory than you, and this is frequently my problem, that people know me and I don't remember them, but you make some assessment about your behavior, right. As a professor I now make lots of decisions about what I wear on campus versus what I might wear back in my hometown, based on who you think is going to be present or who is actually present and observable to you in that space.

Cameras change the experience of space in a bunch of other ways, though, that I think are really important. One is they actually change the physical boundaries of the space.

We had a researcher install a camera on Sproul Plaza, which is also known as Freedom Plaza, so there was some irony here. And it was to commemorate the sixtieth anniversary of the Free Speech Movement, just to add to the irony. And this camera was capable -- anybody could log onto it. It was capable of zooming in so that you could read not the cover to the book, but you could actually read this (indicating), right, from Russia, for example, right.

And everybody who wanted to could log onto this camera. And you could pan, tilt, and -- pan, tilt, and zoom. And you could take pictures and post them on the website, up to five pictures a day. And people took really interesting pictures, as you might imagine on a college campus.

And so one of my least favorite photos is this photo of a woman taking kind of like a Penthouse spread, if you can imagine, because they zoomed in on her from the top, while she was reading The Crying of Lot 49, just to really round it out for you. And this whole conversation ensued about how, well, she's really been waiting for us to take her picture all of her life because she knows she's in public and she's posed this way. Now of course in order to get into that particular position, to take this picture, somebody would have literally to have been straddling her, at which point they probably would have found themselves in the fountain, right. Because when people are present in a physical space with you, you're unable to engage, right, you might not have a legal protection of privacy, but you have these other things called norms and self-help, right. And so perhaps this person would have found themselves kicked someplace kind of unpleasant. Or perhaps they would have found that there was a little bit of social censure, you know, that people didn't actually want to be straddled and have their picture taken in this particular way.

But because the technology meant that this person could take this picture from, it was actually Estonia, I think, right, that the whole boundaries of the physical space, it wasn't Freedom Plaza which is defined by, you know, the Student Union building on one side and Bancroft Avenue on another side, it all of a sudden was Russia. Somebody's bedroom in Russia, right. So the physical boundaries of the space are all of a sudden.

The temporal boundaries of the space are lost, too. So when I expect I have no privacy, I have no privacy vis-a-vis the other people who are there. The other people who saw me. I don't expect to be present in this space 3,000 years from now, right.

And if you -- like Tara Lemmey I'm sure remembers this, but on the internet people participated in news groups. And all of a sudden DeJa News came along, right. And so somebody was sucking up all of the posting of news groups and archiving them forever.

And there was one segment of the online population that went nuts. They were like: Oh, my God, this is an outrage. This is an affront to my privacy. And there was

another half of the Web that went: Are you kidding? That was a whole -- it was all a public discussion. Of course it can be archived, right.

We had this understanding of social forgetfulness, right. People and machines do different things well. People notice the people that they know. They notice things they're looking for. Frankly, when I leave the room today many of you I could never pick you out again in a crowd, right. But machines are actually really good at that. They may not be good at facial recognition, but they are good at different kinds of pattern recognition. They're getting better at gate recognition.

And so we -- this temporal boundary, all of a sudden your presence in the space could be remembered forever, right. We are reaching the point where storage costs nothing, right, David? That's it.

So, you know, when Dr. Norris talked about we can't acquaint my eyes with the capacity of these digital network surveillance cameras. It's kind of like saying the stick with the point on the end is the same as the Uzi, right. It just doesn't make sense. Yeah, they're both weapons, you know, but the magnitude actually does matter.

And right now, you know, we have no laws with respect to visual surveillance at the federal level. We just decided not to deal with it. We're seeing these quirky little laws pop up at the state level that say, you know, you can't use your camera phone to take pictures of people in the dressing room or in the locker room or on the floor of the gym or you can't use them in lots of office buildings, right. Not because of law but because people don't want their trade secrets walking out the door.

And so, you know, we need to deal with both, I think, a richer development of norms but law has to play role specifically when it comes to ordering the relationship between citizens and the state. And I don't think it's an easy process. I think it's harder than dealing with electronic communications, but I think it's one that we have to start on now.

MR. BEALES: If I could just ask the panel a question about something that the Committee saw yesterday. We toured the airport at San Francisco and there are numerous cameras throughout the terminal and throughout the facility. Lots of them are sort of perimeter security. And, you know, watching places where it would be inconvenient to have a guard nor a substitute for a policeman in that regard.

And some of them are essentially watching the volume of traffic in lines to clear security in different places, in order to move people around to make the experience better for users.

Now obviously incidentally there is a potential for surveillance that comes from that, but the main justification for the -- you know, for the camera, for somebody watching

is to improve the user experience and to, some extent in some of the application, to be a remote where it's not feasible to send a person or it's too costly to send a person.

Do you see a distinction between that kind of surveillance, you know, where any -- where any real surveillance of a person is completely incidental or more likely after the fact and the surveillance that's installed for surveillance?

MS. CONEY: Well, it's interesting that when something is initially deployed it may be deployed for a particular purpose, a very narrowly defined use. But if it has use and can be adopted for use for other things, then you have this term "mission creep" come into play.

If a technology is being considered for a particular purpose beforehand, what's the process for reaching that determination, is it something that is coming as anecdotal. We think this is going to accomplish x, so let's do it. Or is it based on an analysis, a review saying this particular technology is going to be well suited to accomplish this. Do you continue to evaluate that?

Do you have weighted on that an auditing process that will make sure that indeed the images that are captured are specifically used for the purpose for which it was reported that this technology would be used? And are you reasonably sure that in this audit, the audit is done not using the same people who lobbied for the funds to be used or are currently monitoring the technology? Do you have a sufficient check and balance to be sure that that is in fact what this technology is being used for?

And then looking at the long-term storing of the data, if it's only used to monitor traffic that's coming in and out of the airport for this particular day, did you need it a week from today, and then is the technology sufficient in obscuring individual faces, unless it's in need or a reason to have more detailed information retained; is that the case?

The whole analysis review, use of the technology, and then constantly monitoring, at least reviewing how the technology is used to be sure that it's in fact being applied in the way that it was intended to be applied and that it's actually provided some kind of benefit. And then the public is aware that the technology is being deployed and then there is added insurance to be sure that it's not being misused or abused in some way and that there are adequate penalties if that is the case.

MS. MULLIGAN: Yeah. I mean I think, right, if somebody came to me and said, 'I want to use cameras to deal with traffic flow and traffic control,' I would say, 'Great. Set them at a resolution so that you can tell how many people are there but you can't tell who they are.' I don't care about it. It serves your purpose. Nobody's going to come and ask you for that data later on because it's useless.

And there are researchers, Latanya Sweeney at Carnegie Mellon has done a bunch of research about different kinds of pixelations that you can use to blur images. There is

some research going on at U.C. Berkeley about respectful cameras. Can we figure out visual cues that tell cameras not to record faces but record other parts of the visual landscape.

And so I think there's hope that technology can actually provide some of the answers so that we can actually use some of the technology to gain this kind of benefit, right. Clearly I'm not opposed to cameras in all spaces. They're useful for a whole host of different things. It's can we make sure that they're useful for the purpose for which we choose to use them, but don't, you know, create kind of unintended consequences.

I think when the deployments are, for example, for law enforcement purposes, that that balance becomes much finer. But I think there are a whole host of applications where it's probably quite easy to craft policies and technologies that respect them.

MR. BEALES: Yeah. How about that?

MS. WONG: It's going to be so boring if we all end up agreeing, but probably that's actually going to be the case at least here. The only thing I would add is, because I come at it from like how do we design products, and I think it goes based on sort of what the Federal Trade Commission said are good privacy principles: What are you collecting; is there a justified need.

And that goes to what you were talking about. For me, when I look at products, the devil is in the details. If once you implement, how do you deal with it. So who's training those officers about how they can use that product?

Not only should the product have built into it low resolution, maybe it doesn't store at all if it's only crowd control. But then in addition to that the training of the people who are using the technology and have the position of monitoring the traffic, but that's what the limitation of the technology is supposed to be for only, need to have that training and you need to follow through on that part of it. So that's my only add.

MR. BEALES: Joe Alhadeff.

MR. ALHADEFF: Thank you. I guess this question could be anyone, but it was originally thought of for both Deirdre and Nicole to discuss because you both talked in one way or another about the wiring of public spaces. And I'm actually looking at it from a non CCTV point of view because I have remained successful in avoiding that topic.

So the question I had is we are now wiring public spaces with the government providing funding for internet access and other types of telecommunications access in public spaces. And does the role and the involvement of the government in that access in the public space change the character of any of our privacy expectations or in any way impact what our are expectations of using technology we are familiar with in private spaces but now in the context of public spaces?

And I say that in the context of the earlier comment that was made about the virtual border. And so I was just wondering both of your impressions since both of you are involved in different parts of, aspects of this kind of wiring how you view that. Thank you.

MS. MULLIGAN: Well, so, you know, the primary privacy law that would be operating there would be the Electronic Communications Privacy Act. It turns more on whether or not you're offering a particular kind of service to the public. And so, you know, the government vis-a-vis its employers or a private company vis-a-vis its employee -- sorry, excuse me -- you know, has one set of rules. But to the extent whether you're the government or the private sector and you're offering a electronic communication service to the public, I think the law would apply pretty much the same way.

I'm happy to stand corrected if I'm wrong because I haven't actually thought about this particular hypothetical. I think there are different issues, so that even under the statute the ability to use data for internal purposes is far less regulated than the disclosures of it. And Google operates in this environment and has done all kinds of things with that particular flexibility in the rule, so I'll let Nicole talk to you about that. And I'll let you...

MS. WONG: Oh, it's a terrible handoff. I see what you're talking about. Our involvement along with Earthlink about the wifi project here in San Francisco or Mountain View in offering free wifi. It's a project that we're really excited about in terms of expanding access to the internet for a wide range of users. In terms of does the government's role make a difference, I agree with Deirdre in the sense of the content, the packets, the IP addresses. Those are run on our servers and so governed by the ECPA. And if the government wants access, my sense, and of course we don't have -- we haven't won the wifi project in San Francisco yet, but my sense is that we would be governed by the ECPA and access to the government would be along those lines, requiring legal processes dictated by the ECPA.

MR. ALHADEFF: I guess actually I was less concerned with the government desire to access the information with a warrant or appropriate process after the fact and more the concept of does the government, because it in some cases in some city deployments is actually funding completely the access, do they then get the right to create policies that define the privacy expectations of the space, was more of the question I was talking about and whether there was a view related to that, rather than, yeah, I would assume that the law as it applies still applies in that purpose.

I was just wondering whether the government has changed its societal role in creating the privacy expectation of that space all of a sudden. MS. MULLIGAN: And is your question there more about for the example, if there are kind of forum kind of spaces or -- because, you know, part of it depends upon what the function is that you're engaged

in, right. You could be using it for email. You can be using it for a blog. You could be using it to create a website. And your privacy expectations would be different there because of the activity that you're engaged in and because of the legal framework. So are you looking at the kind of public spaces that the government might create within the network?

MR. BEALES: Or, Joe, is this -- the way I interpreted the question is could the government make a rule that said if you go to adult places, we can monitor?

MR. ALHADEFF: In some cases it's the government all of a sudden becoming a quasi ISP or surrogate ISP in some of these cases and does that create a different expectation of privacy or should -- should there be a different expectation of privacy?

MS. MULLIGAN: Go ahead.

MS. WONG: That's a great question. I have not been in all the meetings involving the WIFI project, so I don't know that that has even been raised. I think that part -- some of the bidding ha to do with like what's the service that we purported to offer and can we protect it from spammers and people who would send viruses through the service and that sort of thing. Things that you would expect your ISP provider to do.

I have not seen the city try to assert either a content-based type of regulation or limitation or surveillance. And I'd actually be concerned about that.

MS. MULLIGAN: So on the content side, I mean the government would actually face deeper trouble than a private company, right. The private companies are pretty free to filter and block what they want within the limitation. You know, they might face some kinds of challenges, but to the extent that the government started deciding to make content decisions on behalf of individuals, that would be more likely to be challenged even in their role I think as a kind of quasi ISP.

My understanding here is that most of this is done through kind of a contractual basis. It's a funding. And so I think that the companies are still going to be in the policymaking role.

On the privacy side, no. I don't -- you know, I don't think ECPA doesn't provide a lot of flexibility for the government to step in, I don't think, and say, well, we're going to do x. I mean clearly an internet service provider has some flexibility to offer different kinds of services that raise different kinds of privacy issues.

And I think you can imagine if the U.S. -- if San Francisco decided that they were going to run their own Gmail service and they were going to read all of our mail, people might feel a little bit differently about than Google, maybe. But, you know, -- does that answer your question? Okay.

MR. BEALES: John Sabo.

MR. SABO: This is sort of a practical question. Walter Lord, you know, did all those books on the Titanic and one of his chapters was "Did Ships Get Big for Captain Smith," implying that Captain Smith was a sailor who graduated to be the captain and simply couldn't handle the technology. And there were all these other issues like inadequate binoculars and regulations and so on.

But isn't that the same thing we're dealing with here? As a practical matter, you have a grant tsunami. You've got innovative companies, Google and others, who are like looking at the marketplace and determining what makes sense for them in terms of revenue and growth and their customers. And they're not bound by -- of course they have corporate policies, but they're really looking at the marketplace. And you have government, and now add a terrorist environment, basically exploiting every available tool that it can to accomplish what it views as its mission.

Then you have the technology providers themselves who are building incredible technologies at huge rates. Aren't we really entering into a Captain Smith situation where we can have all the public debates that we want, but without a set of practical, definable controls that might be agreed upon both by the private sector, by the technology developers, and by government, we really aren't going to get anywhere. We will be in a reactive mode. We'll be deploying technologies that will likely be utilized and exploited and leading to unintended consequences. So that's my little preamble.

And my question would be: Let's say we have, you know, a year. As a practical matter, what is it really possible to do? You're not going to raise grand public awareness because the technologies are not widely deployed yet. So you won't have huge breaches, like we had with data breach. What can we do over the next year as a practical matter, accepting the realities of the marketplace and the realities of government drive for and hunger for more data and surveillance and so on for legitimate reasons, to move towards a greater sense of getting our hands around this? Is it a set of standards, best practices? Can you form a small coalition to deal with some of the issues or is this really impossible to manage? Just a quick response.

MS. WONG: Let me take one shot at that. I think it's all of those things. I think responsible companies do and should and are, in fact, getting together to talk about what are the best practices for Web 2.0, for being the repository for so much more information. And I think that we are also as a group going to our legislators or, for example, in the meeting with the attorney general a couple of weeks ago, talking about our serious concerns about government access to that data and what is appropriate and what isn't.

So I think it's a couple of things. I think it's: A, the companies themselves establishing the best practices. And, again, from our perspective, having practices that are protective of our users' privacy is key because our next competitor is only a click away. So if we can't retain our users' trust, we know that it's pretty easy to lose them.

In addition to as an industry getting it together, I think we are incumbent to reach out to government at the law enforcement level, at the policy level to move the ball forward in terms of things like federal legislation that truly is comprehensive, baseline consumer privacy legislation, something perhaps more in line with Europe. And there is a group that's working on that now. And to address the serious issues and the flaws that we've touched upon a little bit with current government surveillance laws.

MR. BEALES: Our well known author Jim Harper.

MR. HARPER: Nicole, you probably read and reread California Banker and Bankers versus Schultz and U.S. versus Miller every morning, but for those who don't, those were mid-'70s cases that essentially ratified the Bank Secrecy Act requirement that financial institutions should collect data about their users. And then in the Miller case the court said that those were just business records, and so individuals had no Fourth Amendment claim to those records.

If that is the general rule, that stares your entire Web 2.0 business model right in the face. The courts -- I did a search in under a quarter of a second using your handy service up here -- and the court said: "The depositor takes the risk in revealing his affairs to another that the information will be conveyed by the person to the government," end of story. No Fourth Amendment claim and information that you hold.

Because your business model relies so much on having people put personal, private information in your hands, I'm not impressed by talk of statutes or talk of practices or anything else. What are you doing to reverse that pernicious rule in the Supreme Court?

MS. WONG: Watching it carefully. Trying to be cognizant. And, again, as I tried to describe in our process as a company, really looking at whether or not we are doing our part in terms of creating products that are good for user privacy that are keeping it secure, being extremely cognizant about requests for information, whether it's requests in civil litigation, requests from the government, sharing with partners -- and we don't, as a general rule, do that unless it's necessary to complete some sort of transaction on behalf of the user. So I am cognizant.

And Deirdre actually wrote a tremendous article identifying that business records issue. I don't have a particular piece of litigation to bring to counter that in the Supreme Court. I think we just as a company watch it very carefully inside.

MS. MULLIGAN: Just since she teed it up, I mean I think you're right, that the business records cases have been read quite broadly, but I think they've been read quite broadly sloppily. The cases at issue, they involve not just business records but they involve business records that the entity to whom they were being disclosed actually had an independent interest in, right.

So the banks need the information on your checks to actually clear your checks. And there's a distinction between the record of me opening an account at Google to store my personal stuff, right, think about it as a storage locker. You can equate that account-opening information I think with the business records that were issued in that string of 1970s cases that just stink. But I think that the stuff that's stored at Google is much more akin to the stuff that you store in a locker, a storage locker.

And the Fourth Amendment case law is actually much stronger around that stuff. And I think that ECPA used the wrong starting point for that discussion, but I think there's still hope that we can reverse that conversation with respect to Web 2.0.

MR. BEALES: Joe Leo.

MR. LEO: Thank you. My question is I'd kind of like to reverse the paradigm for a moment and get into the issue of opting out and the legal rights of opting out. For example, for Google to say to the government, 'No, I'm opting out. I'm not going to gove you the data because there's been nothing in my system that violated a law of misuse.'

Secondly, and we heard earlier about installing up to 50 million cameras in Britain over time. Clearly that's more than monitoring whether I ran a red light or not. Yet in this country we kind of, like some states have said you can't put a piece of glass over your license plate to block the camera from recording your number, but could you do that because there are 50 million cameras and you're not running the light, so can I opt out?

Or, and lastly, in looking at the public space, can I go to a great masquerade ball and wear a mask through the public space, and I haven't done anything wrong, so that I know there's cameras there, but I'm not interested in them knowing who I am at a public space, conducting myself otherwise in a lawful manner?

So the whole question I have is the right to opt out. Assuming for a moment that we're not that successful in writing brilliant legislation to give us more freedom rather than less, so could the panel or whatever address the question of opting out, legal opting out?

MS. CONEY: I love the fact that you asked about this whole issue. The privacy community has been very strong and especially those who come from a consumer privacy protection perspective. Opting out is not the model. Opting in is the true consumer privacy model, that you volunteer to participate in something, fully aware of what your options are, what your privacy rights are, and you agree to share this information -- your personal information for that specific purpose.

There's something called Fair Information Practices that pretty much govern what the privacy rules are or what the privacy rights are. Are those consumers, are those engaging in information transaction or transactions that require the exchange of information. The Federal Privacy Act is written based on Fair Information Practices. It's

not, you know, the best, but it definitely has some of the key components that assert the privacy rights of citizens, because each agency that collects personally-identifying information on its citizens have to have rationale for doing that, have to provide access to that information, and a right of correcting incorrect information, and be sure that they secure that information and it's not used for purposes for which it was not collected.

The only options for getting out of that is if it's for national security or it's in the conduct of a criminal investigation of some type.

Taking the same principles for Fair Information Practices and bringing it out into the marketplace has been a hard struggle to get those principles adopted and accepted. Most industry, most private sector actors who collect personal information like the opt-out perspective. That they have the information and you have to figure out how to tell us not to use it or not to contact you, or that kind of thing, working in the public space to educate consumers about this, working to provide information to policymakers about the importance of providing the right of consumers to control who collects information and how that information can be used. And as we move to a more digitized online experience it will become critical to assuring privacy and fairness in the commercial space and privacy and civil liberties in the public use of information.

That's, you know, key component and one that should be a part of the discussion.

Now as far as cameras in public space and how that's used, that has to be part of the overall discussion about why we're using this technology and what are we going to accomplish with it, and is it realistic or is it not. And, believe me, as you see more cameras pop up, eventually they're going to catch something interesting on film, and that will become the impetus for saying what's the right choice and it was something we should do and what not to do, and not have it based on real analysis and real study. And that would be unfortunate.

MS. MULLIGAN: My husband's a photographer. He's a photo editor. And taking pictures in public places, he's been a news photographer. And you don't typically ask people for consent, right. You take their picture. That's his job.

Of course he's also gotten hit in the face once in a while, had his camera ripped out of his hands and the film taken out, and some other things. But, you know, as I said, the understanding of capturing visual images in public places is complicated because of kind of an access to information. You're engaged in public behavior. You're in a public place.

And so while I think I agree with Lillie in many respects with respect to kind of the role of opt out, I think when we're talking about photographing people in public places, the conversation gets a little bit more complicated. I think with respect to the government it's actually a little bit more straightforward. I don't think opt out is really a meaningful thing, right.

If we give -- if we decided as a community that we needed to deploy cameras in airports, for example, for safety reasons, it really wouldn't be great if we let some people opt out. Because the people who opted out would be the problem, I think. Or, you know, at least some of them might be the problem. I might opt out too, but at least some of them would probably be the problem.

But I think with respect to -- you know, the conversation that we haven't had today is the fact that along with surveillance by the state, we have this whole movement of what's called sue-veillance, right. So it's watching from underneath. It's everybody out there at the Republican Convention capturing their own competing images of what happened and using them in court to dispute the official version of the story.

One of my close friends runs an organization called Witness which arms human rights activists with technology to go and film and photograph human rights abuses. So, you know, technology plays an important role in altering the power and balance because it allows the public, in fact, to kind of monitor the behavior of government.

Photographs, like reporters, have been a crucial kind of vehicle for holding the government accountable. And, as I say, a picture is worth a thousand words.

So, you know, this is a complicated conversation and so with respect to kind of citizen-to- citizen image taking, you know, our whole tort law hasn't really evolved very well to deal with all the different kinds of images. You may have seen HotorNot, or there's MobileAsses.com, right. There are a lot of people taking pictures that are not quite right out there. But it doesn't necessarily make them actionable. And I think that our norms and our law haven't really dealt with the changes in technology on a whole host of dimensions.

MR. BEALES: Well, this is a fascinating discussion -- oh, I'm sorry.

MS. WONG: That's okay.

MR. BEALES: Go ahead first.

MS. WONG: I'll be really brief, because I wanted to address from sort of the company side the notions of opt out. And I think for us as a company in trying to deploy the best possible services to our user, we really take it service by service. So, for example, our Google Web Search, which is our flagship service, if you will, you can use that with complete anonymity in the sense that we don't ask you to register with us before using the service. You don't have to have a cookie.

But you should know when you come to the site you will, by default, get a cookie and that cookie is for the purpose of remembering what language preference you want to view our site in. Remembering if you've set Safe Search, which filters out inappropriate content. That when you come you aren't going to see that. And we find that to be a better

user experience for our users. That if you had to reset your preferences every time you visit our homepage to do a search, you wouldn't be coming back that often.

Having said that, we believe in the choice, which means that we do offer the service allowing you not to use the cookie, allowing you not to register. And if you register you get the bumped you, Personalized Search, which is probably going to send you better results, but maybe that's not as important to you as preserving some of your rights of privacy.

So for us, for our purposes the issue is how can we deploy the best service and do so in a way that gives the users the best choice of controlling what information they want to give us.

MR. BEALES: This has been a fascinating discussion. I want to thank you all for being here today. We really appreciate it, and I wish we had more time to explore this.

Unfortunately we have on our next panel a guest who has to leave at 3:00, and so we need to cut off this discussion and move onto the next panel, which is also interesting and central to a lot of the work we do. And that is Identity Authentication.

And because our first guest has to leave early we'll do this a little differently. We'll hear from him, we'll ask questions for as long as he can stay, and then we'll go to the rest of the panel and have questions at the end.

PANEL - IDENTITY AUTHENTICATION

MR. GEORGE VALVERDE, CALOFORNIA DEPARTMENT OF MOTOR VEHICLES
MR. JIM DEMPSEY, CENTER FOR DEMOCRACY AND TECHNOLOGY
MR. JONATHAN FOX, SUN MICROSYSTEMS

MS. SOTTO: Thank you very much to our next panel for being seated. I will go ahead and introduce our speakers in turn before they speak.

We'll start with our first speaker, George Valverde. Did I pronounce that right?

MR. VALVERDE: Yes.

MS. SOTTO: Okay. Mr. Valverde is the Director of the Department of Motor Vehicles in California. He was appointed by Governor Schwarzenegger on March 23rd, 2006. Previously he served as Undersecretary of the State and Consumer Services Agency and before that was Deputy Secretary for Fiscal Operations.

Thank you for joining us. The floor is yours.

MR. VALVERDE: Thank you very much. You know after listening to that discussion it put my position in a broader perspective, understanding, appreciating the role and responsibility we have in the Department of Motor Vehicle here in California. I

want to start out by giving you a little bit of the scope of responsibility of the Department of Motor Vehicle. And bear with me. I've been with the department a little over two and a half months.

Now what I found out is that in California we register -- or we actually issue driver's license of -- to 25 million drivers, or ID cards. We have over 30 millions vehicles that we register. I have over 200 field offices throughout the state of California. So just to give you an idea of the scope of responsibility that we have here at the department.

Those driver's license, most individuals have to renew every five years. Vehicles have to be renewed annually. We see on an annual basis in field offices alone 2.5 million people. That's how many people are coming into our field offices.

In terms of Identity Authentication, the Department probably has been engaged in some form of verifying identity within the last 10 to 15 years. I asked our staff to give me some idea of what kind of authentication do we do. Legal presence began, for example, in 1994. And we do this by verifying that a person's identification is consistent with where they say they are from.

You know we currently have an INS connection through the Systematic Alien Verification and Entitlements Program, the SAVE system, which became effective in 2005. As of 1999 we began validating true full names. And what we did is basically go through our database and assess those names that appeared unusual or different and ask those individuals to validate, you know, is this your true name. For example, the Santa Claus, the Spider-Mans. We suspected those may not have been their true full names. So through that system we've tried to valid true full names.

We also verify that with the Social Security system and try to ensure that we are identifying an individual that they are a customer through the Social Security verification system.

Other things that we do is new drivers. As they come in and they bring in their birth certificate, we will have two individuals in our field offices, you know, a new registrant for a driver's license, we will have two of our driver's license technicians in the field offices validate that, you know, you are who you say you are. It's more of an internal check, one, to ensure that we are not issuing invalid driver's license or that our employees are not issuing fraudulent driver's license. So we attempt to do that through that process.

We are also in the process of assessing what the impact of the Real ID may be on the state of California. We have initiated a steering committee that is incorporating the various state entities that may be impacted by the Real ID. We have begun discussions with Homeland Security and with our congressional delegation and our governor's office in Washington, D.C. relative to the cost, the implementation timeframe, and some of the

significant concerns that we have relative to the information that we are going to be faced with.

Based on preliminary information, we expect the cost of attempting to address the Real ID to be upwards of $500 million. And this is just based on our knowledge today. We understand the regulation has still not be published and, you know, that's still subject to change.

We also expect that we're going to see upwards of an additional 2.5 million people coming into field offices. So if you think about the numbers I mentioned earlier, that we currently have 2.5 million people that are currently coming into our offices, we're going to double that number starting in 2008. The third consideration is the documentation that we're going to have to retain and developing the systems, the capability, and the -- you know, the verification capability to validate that information.

California is currently in the process of upgrading our archaic legacy system. That represents a seven-year IT project that is coinciding with our efforts to comply with the Real ID. And so in many respects we are faced with this perfect storm, where not only do we need to upgrade out information technology systems but we're being faced with a major policy and program change that we are going to be faced -- you know, have to address beginning in the next two years.

So while I'm not in a position to tell you exactly how we're going to deal with all these considerations today, I can tell you that the Legislature certainly has been receptive to some of our concerns, we've had hearings on both our information technology modernization program proposal. We've had -- just recently the Legislature, at least preliminarily, has authorized expenditure authority for '06-'07 that would provide us with resources to begin the planning and begin some of the infrastructure work that we need to begin consideration of what the Real ID may mean to the Department of Motor Vehicle here in California.

With that, I'll be happy to take questions, comments, or any thoughts you may have.

MS. SOTTO: Jim Harper.

MR. HARPER: Thanks for coming down to speak with us. Appreciate hearing from you and I appreciate your preliminary thoughts on Real ID. You may not have been here in the morning when I announced a book I've got out on identification, and there's a chapter that deals with the Real ID Act specifically, concluding for the most part that these are reforms that do not fix. In fact, they change processes a lot, but don't fix the underlying problem with our identification systems.

But sticking to Real ID, I've been up to New Hampshire a couple of times recently where they had a very serious debate about a bill to decline the state's participation entirely in Real ID because of its potential or its actuality of being a national ID.

One of the terms of debate in New Hampshire was the fear of state officials, that the federal authorities would deny New Hampshire travelers access to airplanes. They would be unable to travel due to the way that the Real ID Act tries to coerce state participation.

So I just want to ask you, when you get to that, so you'll have this in mind when you get to that point, do you think that the federal government would prevent Californians from using air transportation if the state were to decline participation in Real ID?

MR. VALVERDE: Well, I'll tell you what I understand. Actually I haven't put -- I haven't thought about what the federal government may or may not do, but my understanding is one of the intentions of the Real ID is to allow compliant states who issue the Real ID card, whoever these individuals are, assuming California were to comply with all the provisions of the Real ID, would provide the authority then to access commercial airlines.

You know, I'm assuming, and I think the Legislature is reserving the right to exercise some policy judgment in the next -- probably the next legislative cycle over what or how California may comply with the Real ID.

MR. HARPER: Do you think -- I'm sort of asking you to guess about how politics works, and economics. Do you think the federal government would essentially shut down the economy of the state in order to coerce your state government to do what it tells you? Go ahead and say probably not if you want to.

MR. VALVERDE: I will reserve judgment on that one.

MR. HARPER: Thank you.

MR. BEALES: Jim, you have low expectations today for everybody.

MR. VALVERDE: I appreciate your consideration, though.

MR. BEALES: Joanne.

MS. McNABB: Thank you. As you described, the types of documentation that are currently required by California DMV in order to get a license, they're very -- but they're essentially the same requirements under Real ID with perhaps a couple of changes as well as many of the security measures, I believe.

What -- do you think that Real ID would make -- requirements would make our driver's licenses more secure. That is, better representatives of identity, better indicators of identity?

MR. VALVERDE: Let me answer this in a different way. I'm committed to making our identification cards and driver's license as secure as possible. And I'm saying that because regardless of how or when we are asked to comply with Real ID, I think California is intent in ensuring that the driver's license that we issue is the most secure identification or driver's license that is -- that we can -- that we have available.

Currently we're in the process of issuing a request for proposal for the next generation of identification cards and driver's license. Our expectation is that we are probably going to be looking for a higher level security in that particular identification card.

Now whether or not -- you know, my assumption is, say, that will be compliant with Real ID, if there are provisions that we're required to comply with there. But regardless of that, our intention is to provide a higher level of security in what we issue.

MR. BEALES: I'm sorry. Lance Hoffman.

MR. LANCE HOFFMAN: I'm aware, apropos of Jim's question, that California at least used to have the seventh or eighth largest GDP if it were a nation in the world.

MR. VALVERDE: I understand we're fifth now.

MR. LANCE HOFFMAN: You're fifth or sixth now? So it's interesting what would happen in his hypothetical. Can we learn from California at the federal level? Do you have -- this is a process question, really. Because actually I didn't get a chance to ask a question of the previous panel, but it struck me there also that it might be a good idea, and we talked about this earlier, about having some more public examination of whether the proposed program, whatever it was, was going to be effective, whether it was cost-effective and that sort of thing.

Do you have in California requirements for a public -- either a public cost-benefit analysis or a proxy impact assessment for various programs including your program? Are they subject to peer review? Are there public comment periods? Or do you just sort of do like some agencies of the federal government, just implement them and try to figure out what's going on later?

MR. VALVERDE: Well, I would say that annually I'm subject to that because the Legislature reviews my budget on an annual basis. And through that process they're evaluating, you know, the Department's performance, new proposals that are being considered, the value of those programs, whether there is a benefit in programs that are being proposed.

As I mentioned earlier, we had proposed, you know, through the governor's budget upwards of $18 million to begin the planning for the Real ID. And much of that planning is in terms of our information technology infrastructure. That was scrutinized by our Legislature and has been modified relative to focusing the attention on that, not so much on implementing aspects of the Real ID but in implementing the information technology that will allow us to drive some of our services that are currently performed in field offices, you know, onto the internet that will allow you, say, to do your renewal of your driver's license, do your vehicle registration and change your address, for example, via the internet, therefore avoiding a visit to one of my field offices.

MR. LANCE HOFFMAN: Did those changes come about -- presumably you submitted one proposal and there was some pushback, or can you do it this way instead of that way, or something like that, where did those changes come from? Were they in a public process or...

MR. VALVERDE: Absolutely. Through the Legislative Budget Committee Review Process.

MR. LANCE HOFFMAN: Were there public hearings or –

MR. VALVERDE: Yes, there were.

MR. LANCE HOFFMAN: There were? Okay.

MR. VALVERDE: Yes.

MR. LANCE HOFFMAN: Thank you.

MR. BEALES: Ramon.

MR. BARQUIN: I have two questions. I think they're somewhat related. First, you did mention the -- if someone shows up with a birth certificate, that you would send two people out to try this. And that raises the question of the breeder documents for identification feeding into the driver's license as then, you know, the closest thing that we have to that national identifier.

The first question is has the State of California looked at the breeder documents themselves in some way to try to address that specific need? And the second question that's related has to do with data integrity. Any comments on -- I was struck when you said, well, you're checking for the weird names like Spider-Man and Mickey Mouse, but in the state that has such an incredible diversity of multiple languages with multiple scripts and whatever, that must really create a very significant issue for the database that you run.

MR. VALVERDE: It does. And it is one of the issues that we're going to be looking at. What I -- what we have established through our Steering Committee on Real ID is

working groups. I have four distinct working groups. One of them is looking at policy and legislative issues. Another one is dealing with more programmatic concerns. We have one on IT concerns and one identity and security. And I'm thinking that that particular issue will be addressed within that context.

With respect to name fields, I can tell you, and this is something I learned as I became more acquainted with our DMV, that historically we've only captured 34 characters in the name field. So you think about, you know, some of the names that we see today, you know, our name fields are not sufficient to accommodate that.

We've had to truncate names in order to put them within our name field database. So certainly that's the first thing I need to do. We're looking at expanding our name field characters to 175. So that's -- so your comment is, you know, well taken. And that will be something that we will endeavor to do within the next year, regardless of the impact of the Real ID.

MR. BEALES: Mr. Valverde, thank you very much for being here. I'm sorry about the confusion about scheduling, but I'm glad that you were able to be with us.

MR. VALVERDE: I appreciate the opportunity. And if I can come back at some other future date, I'll be happy to do that.

MR. BEALES: All right. Thank you.

MR. VALVERDE: Thank you.

MS. SOTTO: Jim Dempsey, thank you for joining us again.

Jim is the Policy Director of the Center for Democracy and Technology, where he previously served as Executive Director. Jim's area of expertise include privacy, electronic surveillance, and national security issues. And Jim heads CDT's international project, the Global Internet Policy Initiative, and is also a member of the Markle National Security Task Force.

Thank you for joining us.

MR. DEMPSEY: Well, thank you. And thank you to the members of the panel as well. Talk about being between a rock and a hard place here, I've got this panel in front of me and Peter Neumann and John Gilmore behind me. (Laughter.)

MR. DEMPSEY: And it's sort of like what can I possibly say that will either add to the discussion or not get me in trouble one way or the other. I think I'll just make a few comments and then take questions. There's certainly more than enough expertise here.

You know, we're in a privacy crisis in some regards in this country today. You know, the elephant in the room is something that I guess I feel I have to mention at the

outset, which is: Does any of this matter if the President can say that he will disregard laws or disregard rules or have two sets of rules?

I think it's incumbent upon this board as an executive branch board to raise these issues as well as the rest of us. It's hard when you're within the executive branch, when you're sort of part of the executive branch, but, you know, you have to ask are we all being chumps if we work hard on compromise and develop some system, something like FISA, something like some of the other rules on intelligence activity, and then the President says, 'Thank you very much. Sometimes I'll follow them and sometimes I won't.'

We also -- if you haven't seen Shaun Waterman's article on the Privacy Act provision in the Senate Reported Intelligence Authorization bill, everybody should take a look at that, basically from what I've read, and I haven't studied it carefully, but it seems the Intelligence Committee has proposed a sunsetted but nevertheless significant amendment to the Privacy Act to allow sharing of information between government agencies exempt from any of the limitations of the Privacy Act.

Now those are not apropos of the topic of the discussion here. Directly, although identity authentication is clearly one of the very, very hard issues on which people are currently spending a lot of time and will continue to be spending a lot of time in the coming years. I think the first step in thinking about identity authentication is to be very careful and precise in terms of the words and the concepts we use. Identity, authentication, verification, and validation, authorization. These can be very different concepts.

I think the best work and the best reference point that I know of is certainly the work done by the National Research Council's panel a couple of years ago and the report that they put out in which they clearly define these terms.

But let me give you one example which I think some of you had heard me say before, but I think it helps illustrate, and again at the risk of telling you what you already know, the Social Security number. The Social Security number is a perfectly good identifier. In fact it's a better identifier than name. There are duplicate Social Security numbers, but there are many more duplicate names than there are duplicate Social Security numbers. As a disambiguator or an ability to tell two people apart, to identify the person, the Social Security number is perfectly good.

As an authenticator the Social Security number is terrible. Now a lot of people have used the Social Security number as an authenticator. That is, they've treated it like a PIN number. An authenticator, as you know, is something that you know, a secret, that is. Something that you have, a physical token. Your driver's license has identifying information on it. It's also an authenticator. It's something you have. You can't print one off quite a Xerox machine, but they have obviously security vulnerabilities, but it's

nevertheless an authenticator issued by a trusted, relatively trusted entity. Or it's something you are. A biometric, et cetera.

The Social Security number is none of those. It's not secret. So many people have it that it's no longer valid as an authenticator. I've actually facetiously, but to illustrate the point, recommended that Social Security numbers should be published, just put them in a phone book. Look them up. And thereby break people of the habit of using the Social Security number as an authenticator.

The notion that you can call up and 'For security purposes, please give us the last four digits of your Social Security number,' that does not prove anything in terms of who I am.

Now it's funny because I think either a phone company or a cell -- some company that I recently had interaction with, which used to ask that question, now has a different set of questions. Obviously, as we all know, it turns out to not be that easy to do good authentication. They asked me a whole bunch of questions about myself that I didn't have a good answer to, until I finally stumbled on the right answer. And then they said, "Okay, we now believe that you are Jim Dempsey."

Now I think that to sort through these issues, I think that this board could do a very good -- make a very good contribution. I think that the document that you produced on technology assessment was a very good set of principles. And I hope it's getting the wide attention that it deserves, although I'm not even sure that this board has fully -- have they fully endorsed that privacy -- the framework?

Okay, all right. You did it quietly. You should have -- that's a good document.

I think that you could produce something similar on identity, that is a guide for both components within this department as well as other government agencies to use when thinking about any system that has an identification element to it. The first question of course being: What has to be personally identified and what doesn't have to be personally identified. Then the other questions being: What levels of authentication are necessary, et cetera.

I was actually thinking of bringing, you know, different identifiers and authenticators with me. I forget to bring my FasTrak thing. But, you know, we all have one pretty good authenticator, you know, bearer of identification today. That's my driver's license.

You know, I've got my business card, which has a lot of identifiers on it, but it's pretty weak authentication. Anybody could print that up easily enough. It's slightly harder to produce the driver's license than the business card.

My D.C. Fare Card, which is a good authenticator, it gets me onto the system. It's got authorization to use the system relatively good. Maybe somebody forges these. It's maybe not worth it. But zero identification value. My FasTrak, on the other hand, has both authorization as well as some form of authentication as well as identification. So we get a monthly printout of when we crossed what bridge and when.

And I think it's really important to sort of sort through with each new system what identity are you collecting, do you need to collect identity, what is the kind of authentication that you have or need for that particular transaction, what are you authorizing, and so on.

There are two possible starting points in that process that I can list offer. One about two or three years ago -- be four years ago now, CDT working with a number of folks including, I think, Richard, you were involved in the Authentication Privacy Principles, which were a set of privacy principles for authentication systems. I think both the Liberty Alliance and Microsoft Passport signed onto these principles as something that they would use in developing online authentication.

Secondly, we recently came out with, as you probably know, a set of guidelines again developed in a multi-stakeholder process, a set of guidelines on RFID technology. And I would only briefly refer but briefly refer at least to the draft paper of a subcommittee, I guess, of this body on RFID and I would say two things, one of which is you really set up an inappropriately short timeframe for comments. I mean if anybody treated the timeframe seriously, it was very short. I assume it's still open for comments. We will submit comments on that in the form of at least our RFID guidelines.

And I think there is in the paper a little bit of not appropriate care given to the use of these terms of identification and authorization and authentication, and so on. But I think that also -- I guess a third point I would make about the paper is I'm not sure it fully follows its own advice in terms of technology neutrality. And I think some of the comments I've seen since about the paper talk about smart cards and contact with smart cards and RFID technology.

I think they all raise roughly the same set of issues. The question is: Is the ability of the technology to respond to those issues but I think it's hard to say one is good and the other is bad, that an RFID is per se bad or that smart cards are per se good. I think it's important instead to look at the issues.

And, you know, clearly -- or at least not so clearly -- to me there's nothing new under the sun in terms of privacy principles. That the Fair Information Principles, OECD, EU, HHS guidelines, that's about as best as I think we're going to get for a set of concepts to think through the privacy issues: Notice, collection, minimization, retention limitations, limitations on a secondary disclosure and reuse, security access, enforcement. Those are

the principles that should guide RFID, contact with smart cards, and the assessment of any other identification technology, again starting with the question of: Do we even need to have identification in this context and how highly need that be authenticated.

I know of five different projects right now that involve identification within the federal government. One is of course Real ID. The second is the Trusted Workers Identification Card, the TWIC. Third is the government workers ID card, which NIST has issued standards for a uniform ID card for government workers and possibly its contractors. Fourth are the passports, the new passports with RFID. And then the fifth is this Border Control Card. There may be others that I'm missing there.

Now I think, and this is sort of my last thought, the technology -- from a privacy perspective, in my view, the technology either needs to remain relatively simple so that we think in terms of the wallet. Different identifiers for different purposes. Different kinds of authenticators. Different kinds of authorization technologies for different kinds of purposes. Cash, for example, is a terrible identifier, a beautiful authorizer. If you -- cash may be the most, you know, privacy-friendly technology around.

But I think we have to either get very simple and remain simple so that we have different authenticators for different purposes or the technology needs to get much more sophisticated if it can ever be able to reliably have different levels, have different information exposed for different purposes, have time limits upon information.

I mean certainly if the music industry and the content industry, generally the intellectual property industry is talking about information dying at a certain stage, we should have identity that dies at a certain point as well.

So it seems to me that right now we're sort of in the middle, which is a perilous place. As I said, you know, being between this panel and the folks behind me, it's a perilous place because I think that we're having -- we're trying to have a little bit of both. And we certainly have the increased storage capacity, the increased log-in capacity. The ability obviously to exchange information now between databases. And that I think is a bad recipe for a privacy with location awareness, trends, obviously with the whole change in the search equation for information that right now I think that we're at a point where far too much information can be collected without the kinds of controls called for under the Fair Information Principles that we've had for now 30 years.

So with that I look forward to your questions or to yield to -- I mean we could go also go to the next one.

MS. SOTTO: Sorry. Confused about format. Thank you very much, Jim.

Our next speaker is Jonathan Fox. Jonathan, thank you for joining us.

Jonathan is the Acting Chief Privacy Officer of Sun Microsystems. In 2000 he assumed responsible for managing customer-facing-privacy issues and co- founded Sun's Privacy Council, which he chairs.

Thank you for joining us.

MR. FOX: Good afternoon. And thank you, to the Committee, for the opportunity to discuss digital identity management and the Liberty Alliance.

What is digital identity management? Digital identity management is a set of business processes and supporting infrastructure for the creation, maintenance, and use of digital identities.

Identity -- digital identity management enables security, controls, manageability, and accountability. Unfortunately, identity management is also a mess in real life.

A typical environment a user has 21 passwords. Forty-nine percent write their passwords down and store them on a file in their PC. The majority use common words for passwords. Sixty-seven percent rarely or never change their passwords.

Password proliferation increases help desk calls, which increase costs. In a non-automated support model, password resets cost an average of 51 to $147 in labor. In an average corporation of 10,000 employees, about 45 percent of help desk calls are requests for password resets.

It is also a world of identity silos. In a typical IT environment ten different ads for services, applications, or services contain identity profile information. Over 80 percent of companies have no identity synchronization solutions. Identity silos are a roadblock to productivity, and bad identity management creates security and privacy risks.

Federated Identity Management is a way to lessen the risk and remove the identity silos. What is Federated Identity? Federated Identity Management is a system that allows individuals to leverage identity elements stored in one entity across several sets of services. It allows for single sign-on and does not require user's personal information to be stored centrally.

The Liberty Alliance was formed in September of 2001 with the goal of establishing an open standard for Federated Identity Management. The Liberty Alliance is a global alliance of companies; nonprofit, government organizations for developing open standards for Federated Network Identity and to offer -- and to offer strong authentication and identity-enabled Web services.

The Liberty Alliance Management Board currently consists of representatives from aol, Ericcson, Fidelity Investments, France Telecom, General Motors, HP, IBM, Intel, Novell, NTT, Oracle, RSA Security, and Sun Microsystems.

The Alliance has grown to over 150 members worldwide, spanning the commercial, government, and nonprofit sectors. Among the public sectors member organizations are: The U.S. Department of Defense, the U.S. General Services Administration, Royal Mail, Hong Kong Post, Canada Post, University of Hamburg, the University of Chicago, and the Helsinki Institute of Technology, among many others.

The goals of the Liberty Alliance are to provide open standards and business guidelines for Federated Identity Management spanning all network devices; to provide open, secure standards for single sign-on with decentralized authentication and open authorization; to allow users to maintain personal information more securely and on their own terms.

The Liberty Alliance vision is to enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of identity information. Liberty's open Federated Identity standards coupled with business guidelines will create the flexible, secure, and open infrastructure that is required to support and manage these online services and transactions.

These are the business requirements it tries to address: Simplified access to services and applications both inside and outside the organization; reduce the need to maintain and manage multiple sets of identity credentials; reduce the cost and complexity of managing identities; enable dynamic creation and management of trusted relationships; preserve privacy and ensure data security.

The Liberty architecture has three components: Liberty Identity Federation Framework, which enables Identity Federation and Management features such as identity and account linkage, simplified sign-on and simple session management.

Liberty Identity Web services Framework provides the framework for building interoperability identity services, permission-based attribute sharing, identity service descriptions, and discovery, and other associated security profiles.

And, finally, the Liberty Identity Service Interface Specifications enable interoperable identity services such as personal identity profile services, contact book services, geolocation services, present services, and so on.

The Liberty Specification builds on existing standards such as SAML, SOAP, WF Security, and XML.

Federated Identity Management makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains. Federated Identity avoids the pitfalls of centralized storage of personal information while allowing users to link identity information between accounts. Since users can control when and how their accounts are linked, shared -- and shared, they retain greater control of their personal information.

In practice, this means a user can be authenticated by one organization or website and be recognized, and deliver personal content and services without having to reauthenticate or share additional or the same personal information.

Federated Identity requires two key components: Trust and standards. The first component, trust, is realized through the important concept of circles of trust. A group of organizations that have established a trust relationship with one another and have pertinent agreements in place regarding how to do business and interact with each other and manage the identity.

Once a user has been authenticated by a circle-of-trust identity provider, that individual can easily be recognized and take part in targeted services from other service providers within that circle of trust.

The second component relates to a common set of technical and business standards and guidelines that allow the development of meaningful Web services. The Liberty Alliance Project was formed to foster the development of such standards and specifications. The Liberty Alliance is not only committed to developing and publishing open standards for Federated Identity but supporting and incorporating other pertinent standards into Alliance specifications. This means businesses can implement Liberty-enabled products and services with confidence, knowing that they will interoperate with company infrastructure as well as the infrastructure of customers and business partners.

Proprietary identity systems may or may not support such standards and thus create technology pitfalls and run away development time and costs.

The liberty specifications were developed with privacy in mind. The decisions made in developing the technology were made to enhance privacy and make it easier to implement good privacy practice, such as consumer consent, consumer choice of identity providers, decentralized or federated storage of personal information and other information related to your identity.

In addition, there are technical features that support privacy, such as XML signature, sign-anonymous access, anonymous access, usage directives, consent- headed blocks, and interaction services. In addition, the Liberty Alliance Privacy and Security Best Practices and Privacy Implementation documents provide guidelines to help companies build more secure, privacy-friendly, identity-based services in compliance with local regulations and create more trust relationships with customers and partners.

I thank the Committee for the opportunity to give these remarks and look forward to your questions. Thank you.

MR. BEALES: Thank you both for being with us.

Jim Harper.

MR. HARPER: I left my card up from the last session.

MR. BEALES: Jim, I've never seen you speechless.

MR. HARPER: Oh, I've got plenty. Believe me.

Jim Dempsey, with reference to the draft report, and I apologize because I was out for the very earliest part of your talk so I might have missed something, I wonder if you have definitions for some of the terms we all use, identification, authentication, and authorization?

MR. DEMPSEY: I mean at the risk of getting it wrong, I think that the best definitions of those found in the NRC Panel Report on Identity. I think the subtitle of which was "Not as Easy as it Seems." But, you know, an identifier is an attribute. An authenticator is something that -- I'm going to get this wrong. So, because again you do have to be precise in using these terms, so I would simply take a look at that NRC report. In my mind it's the best thing out there in terms of helping you sort these things through.

And, honestly, I always have to go back and -- if I'm writing something as opposed to just extemporizing, if I'm writing something on this I always go back and look at that to make sure I got it right.

MR. HARPER: Okay.

MS. SOTTO: Jim, could you provide us with a link to that --

MR. DEMPSEY: Yeah, definitely.

MS. SOTTO: -- report?

And the other thing you also mentioned, while we're on the topic, the Senate Intelligence Committee.

MR. DEMPSEY: Yes.

MS. SOTTO: Shaun Waterman was it?

MR. DEMPSEY: Shaun Waterman's article, yeah, UPI.

MS. SOTTO: Provide us with that.

MR. DEMPSEY: But I'll send to Rebecca both the links to the two CDT products I mentioned as well a link to the NRC report and to that UPI story.

MS. SOTTO: Thank you.

MR. DEMPSEY: Which also has the text of the legislation in it, I think.

MR. HARPER: I'm familiar with that study. It's one of really two writings I ever found that really went into identification theory in any depth. I think the draft report is pretty good on using terminology accurately, but a lot of what is -- a lot of what's

happening in the Department of Homeland Security appears to be non-identifying and attempting to infer identification from the presence of a document, which assuming there's a security context at play, is a mistake.

So it's -- the I-94 program, for example, is very good at tracking law-abiding people, but no good at all at tracking law breakers. And so it provides a wealth of data by the people who you don't need data about and very little accurate data about whom you don't.

But again maybe we can discuss more --

MR. DEMPSEY: Well, I think -- let me say, Jim, that I think that that RFID report, as it goes through, you know, the revision process, is going to be an excellent contribution from this Committee. So I mean I don't have line edits at this time, but I could try to work with you or others of CDT would work with you and Members of the Committee on taking that report a step forward.

I think that one of the interesting things that there's a little bit of confusion about actually is what is identifying personally identifiable information. Again, you're probably all reluctant to jump into the NSA issue, but one of the notions floating around there, one of the defenses I have heard about the meta data side of it, the transactional data side of it is: Oh, well, it's just phone numbers. That's not personally identifiable information, which I think is ridiculous.

But if there is a confusion about what is personally identifiable information and what are identifiers, maybe at that level, if you don't want to get into the specifics of the NSA thing, which I could understand your reluctance to, that might be just a contribution from this Committee in and of itself.

MR. BEALES: John Sabo.

MR. SABO: Yeah. Just a quick question for both of you. One of the key privacy principles and/or practices and legal requirements under the Privacy Act is individual access and the ability to correct information if it's inaccurate, so on.

In automated systems, like if you look at Federated Identity and the services provided, or you're looking at very heavily automated systems where you have multiple interconnections and data sharing, often a lot of that interaction is automated. But your ability to actually access data at a particular database or a particular service provider is then contingent on your authenticating yourself, which may be outside the initial authentication used to access the service.

So as you get more automated, and I think we've already started seeing examples where you're working online, you enter a very primitive but you use an email address and some other little password to identify, suddenly your email address changes because

you've changed service providers and now you're in an endless loop and can't easily change your account. You've got to open a whole new account. And that's kind of trivial for the Washington Post, but that's not trivial in correcting significant data.

I guess my question is as you look at these questions of identity, authenticating identity, how do you address the fact that in order to obtain certain privacy services that ensure your privacy protections you actually need almost an independent privacy authentication and identity regime to make that happen. In other words, you've got to look at more than just the initial service offering. You have to look at the management of your privacy rights in conjunction with identity. I don't know if you have any thoughts about that issue or not.

MR. FOX: Well, at first off, at the Liberty framework the user really does control their identity elements because they are trusted to an identity provider and an information asset system of record. So you have easy ways to correct in single locations your identity information on a rolling basis.

But I agree it is incredibly important to be careful especially in any model with how you share your information and understand the controls in place to protect the information and to manage it.

MR. DEMPSEY: I guess beyond that I would only say that I wouldn't want to see the authentication issue be an absolute barrier to the access principle. I think a little bit the difficulties of ensuring that the requester is the person they claim to be has been used as an excuse not to implement the access people. Again that's not to say it isn't a legitimate concern, but I think it's one we have to work with and overcome with some caution. But this certainly does not undercut the importance of the access principle.

MR. BEALES: Tara.

MS. LEMMEY: I have two questions. Jim, I liked your statement about the either more simpler or more complex approaches, because I think that that's indeed true. But right now we're stuck in the quagmire of the middle. And I'm wondering if you have any predictions about the kinds of things we should do in this quagmire state to sort of pull us back and forth.

And, Jonathan, I had a question for you. I didn't know if you were here for our last discussion about the Web services problem and the Fourth Amendment issues around ownership, if identity followed into that category where this assortment of identity can easily be attained by the government because that hasn't been cleared up under Web services, where does that fit in for you? How have you been thinking about that?

MR. FOX: I should start by: I'm not a lawyer.

MS. LEMMEY: That's okay. Neither am I.

MR. FOX: Yeah. I think that information is always ultimately owned by the individual, the person owns their identity however they choose to share it with various environments. And they have to be careful regarding under what conditions they've agreed to share that information so that they understand the rights that are -- they have agreed to how it can be used.

MS. LEMMEY: So, Jim, perhaps you can also address the second point as well because I think you are a lawyer and you may have thought a little bit about --

MR. DEMPSEY: I'm sorry. Would you restate the second point again?

MS. LEMMEY: In the last conversation around Web services and government access to personal information that's stored at a service provider at a different ISP or at different content companies. With identity management under a Federated approach, those identity aspects would also be stored there differently than if they're stored on your person or on your body. It creates the same challenge, but it creates the same challenge in almost a heightened way around identity, as it does around some of the other content areas we were talking about in the last discussion. And, as well, this simpler-more complex issue. relating -- (Microphone cuts out.)

MR. DEMPSEY: Well, and I think the answer to -- I think I can answer both questions together, because I think they are related. I mean obviously I think we're going to move in both directions simultaneously, that is we are -- I just don't see how we're going to stop getting more complicated with the technology. I hope that complication in this case equals sophistication, which it often doesn't.

I would want to say, though, the thing that's going to push us in the direction of simplification is the bad guys, because the bad guys are going to adapt to the complication and they're going to find ways to piece new forms of controls. Bruce Schneier has written about two-factor authentication in saying that it solves some problems, but it doesn't solve phishing and some other sort of problems.

And so, you know, the bad guys are going to come up with new threats, new -- discover new vulnerabilities and exploit them. Now I hope that in responding to that we can again through sort of a privacy-impact assessment, and that's sort of -- what I would see is that sort of identity-management aspect of the privacy-impact assessment of asking: Do we need to have identity here, what kind of identity, how long do we keep it, is it persistent, et cetera. Those kinds of questions might push you to a simpler solution rather than an increasingly complex solution.

Now, you know, not to keep only referencing things that CDT has written, but we did come out with a report in February addressing the storage issue. Storage, that is networked storage is certainly one of the major trends defining the changing privacy

relationship. You saw the articles yesterday of where Google is going to offer an online spreadsheet function that only works if you give your data to Google.

So for wonderful convenience, for probably free, you will be able to engage in shared work on spreadsheets, but that means you've got to take it off of your desktop and take it out of that relatively- protected communication channel. You know we have both relatively strong protection for data in transit both as a practical matter and as a legal matter. We obviously have very poor protection as a technical matter and also relatively poor protection as a privacy matter for data arrest.

And so what you're doing is you're taking your data, increasingly with Gmail and Hotmail and a whole host of storage services, whether it's Flicker or Delicious or any other network-based information storage, things that used to be on the desktop or, at the very least, used to be at the server in the basement of the building, is now remotely stored and accessible. Where it falls maybe, maybe outside the protection of the Fourth Amendment and in terms of statutory protections enjoys much lower protection than data on your hard drive or your desktop or, you know, I still keep my calendar this way (indicating).

If I used Yahoo Calendars, a totally different set of privacy rules would apply to that. And I think that that and location awareness and the centrality of search are three of the major issues defining privacy.

MS. LEMMEY: So just to follow that up a little bit, with the Federated Identity approach to identity management, aspects of identity become part of that problem. Do you think we have to solve that problem of the ownership issues of information and storage versus business records kinds of things in order to have a better identity system where people are more confident --

MR. DEMPSEY: I think so.

MS. LEMMEY: -- in access control?

MR. DEMPSEY: I think so. I think the answer is going to be threefold. It's going to be user education, it's going to be technology design, and it's going to be policy.

MR. FOX: I also think that Federated Identity Management also changes the equation a little bit. At Sun we have Federated Identity with a ByPAC. Sun acts as the identity provider. I authenticate myself on the Sun side. Go over to ByPAC. It's a political action committee. All ByPAC knows is I am a Sun employee, does not know who I am, knows my Zip code and one or two other pieces of information about me to provide services. But it doesn't know who I am. It does not know it's Jonathan Fox. It just knows it's a Sun employee at my Zip code. And so that by itself changes the amount of information that is being deposited. Because --

MR. DEMPSEY: Yeah, but isn't -- is there somewhere, though, a log? I mean just for systems- maintenance purposes, if the thing breaks you're going to want to go back and figure out --

MR. FOX: It's a pseudonym and it's not stored.

MR. BEALES: To the mic, guys. Not to each other. Sorry.

MR. FOX: It's a pseudonym and it disappears. If you think about the storage issues, even with the diminishing cost of storage, there's still quite a bit of information that's just impossible to store.

MR. DEMPSEY: And I think that's the -- you know, those are kinds of questions that need to be asked each step of the way: What's being collected, how long is it being kept, does it need to be kept. You know, you can do lots of neat things. And partly it's a matter of technologists thinking that through. And, you know, is the neat problem that, oh, wow, let's work on that. Is it going to be: What more data can we keep and how can we use it and what additional value can we draw from it, or how can we provide the service and the functionality without collecting data, without storing data, without having data that can be traced back.

And if you define the problem in the second way, then I think we do have, you know, the possibility for having something that is both simple and sophisticated.

MR. ALHADEFF: And last question. Joe Alhadeff.

MR. BEALES: Yeah, I guess.

MR. ALHADEFF: I guess this was a follow-up to maybe Jonathan's last response. And that was looking at the Federated model, it seems like what you have, if you take, let's say, today's model where I go individually to every website, I provide all of my authenticating information to every website in order to get whatever credential or use of the website I get. It seems like -- and I was just getting -- wanted to see if I was correct in my interpretation. It seems like you have a data-minimization concept in the sense that you may have your choice provider or your identity provider being the one who gets this large treasure trove of information. But then a smaller amount of information is passed along to other people in order to validate whatever it is I need to do at that site. And, therefore, that may be addresses Tara's question to a small extent of: You still have a Fourth Amendment problem, but it may be a slightly more minimized problem because you've limited the scope of the information that's transmitted about you.

I do think, though, that the Fourth Amendment issue may have a chilling effect on some of these things, especially when you consider that external servers may actually be better secured than perhaps a person's laptop, which we've all heard about trojans and botnets and keystroke readers and everything else. And yet you have a trade-off that you

have to have if you want to externalize that information to someone who may be better able to protect it, you are in some cases more legally able to be discovered.

MR. FOX: To your first point, it's both minimization and appropriateness of data. Your identity provider just authenticates you as you. You have other providers who actually are the repository for elements of your personal information. You might use, say, the Post Office for your address and Social Security department for your Social Security number that then are provided at the appropriate time to a service. So it's both appropriateness and minimization of the information.

A couple things. We -- you know, it's important to think in terms of network devices and network identity and how do you best limit data being stored in portable media, so that these issues of things being downloaded out of services don't transpire. There are technologies such as Tadpole laptops which are thin client laptops which you have no hard drive. It's a dumb client laptop where you just get on the network, use the information, the information stays on the server.

So the issue is really the systems containing your data need to be kept secure, and that requires strong security. And we have found time and again security based on open standards and open systems so that there is transparency and understanding and peer review of those technologies provide the strongest types of technology.

MR. DEMPSEY: I would just re-emphasize the point that Joe Alhadeff made, which is that there may be security benefits in remote storage. And I think that it's time for the law to catch up and to be truly technology neutral and to extend to that remote-stored data the same kind of protection that applies to data that you keep closer to your home or closer to your physical possession. Because clearly that distinction is evaporating. And there's no reason why we -- well, I was about to say there's no reason why we would want to stop that trend. There may be, but I think that trend is certainly -- that's the boat we're on right now.

MR. BEALES: Gentlemen, thank you very much for being with us today. We're about to take a break for 15 minutes.

And when we resume it will be with our public comment panel of four people who responded to the Federal Register Notice and indicated their desire to speak to us.

I will call you one at a time and we'll ask you to speak for seven or eight minutes and then give us a chance to ask seven or eight minutes worth of questions. And then we'll have brief public comments from people who have signed up of three minutes each. And that will wrap up the afternoon.

So if we could resume here at four o'clock, thank you all. (Break)

MR. BEALES: Well, it's clear where the real power is. When Becky yells, you all sit down.

Our first speaker today is Mr. William Alsbrooks, who's from Anteon International Corporation.

Mr. Alsbrooks.

PUBLIC COMMENT PANEL

MR. ALSBROOKS: Thank you very much for inviting me to speak here today. Some context for my remarks: I am a computer scientist with over 40 years experience in the design and development of application programs involving large-scale database management systems, nationwide networks, and national security identification applications.

I am responsible for the Credential Technology Group of Anteon Corporation, which is a large-scale systems integrator. Before the end of this week we expect to become part of General Dynamics.

My Credential Group has issued over 40 million secure ID cards: RFID; contract and contactless chips; and optical memory cards, including over one million of the Department of Defense common access cards; over 40 million permanent resident green cards; over eight million border-crossing laser visa cards; and over two million Canadian permanent resident cards.

Today I'm here to talk to you about data privacy, data security, and optical memory card technology as a complement to RFID.

As the Committee's Draft Report correctly states, RFID is not inherently disposed to identification security or to rapid identity verification. RFID can be combined in secure cards with other technologies like optical memory to mitigate for the privacy and security risks identified in the Draft Report.

The operational scenario that US-VISIT currently envisions for the border calls for the use of a UHF, RFID card with a 96-bit pointer to a database, to retrieve a photo and personal data to be displayed on an inspection screen. This scenario assumes that the RFID chip will always read, that the database is always available, that the network infrastructure is always sufficient to return a photo and the biographical data in sufficient time not to impede the flow of legitimate trade and travel.

So in this scenario what happens when the chips don't read? What is the plan when the power fails or if the network is slow or is not available at all?

When an RFID tag or a chip cannot be read for whatever reason, the card must be visually inspected or offline. Therefore, document security becomes paramount.

Is everyone familiar with the expression flashpass? A reliable flashpass is a card that card that can be visually verified to be authentic. You need to be able to verify that the card is authentic and have a high degree of certainty that the card was actually issued to the card bearer.

International forensic document experts have confirmed for me that almost all of the visual security features commonly used to deter counterfeit and forgery have already been compromised or simulated. Many are called out in the draft Report. We use them in our cards and believe them in for a certain degree of fraud deterrence, but with today's high resolution scanners and printers, they can all be faked. And they don't offer the highest degree of document forgery resistance.

The only visual security feature that I know of that has not been successfully replicated or simulated is the embedded hologram in the optical memory card. It is a high definition, two-micron resolution, visual representation of the digital data and biographical data images laser engraved into the optical media itself. DHS's own forensic document lab experts have called the counterfeit attempts at the embedded holograms 30-footers, you can tell they're fakes from 30 feet away, and declared that the optical memory card has put mass counterfeiter out of business. You don't see optical memory cards in the stack of the pictures that ICE displays on the internet.

International forensic security experts verify that data secured on the optical memory cards has never been compromised. The data has not been fraudulently altered.

There are over 24 million optical memory cards on the street right now, issued by Department of Homeland Security, Department of State, and the Canadian government that are counterfeit resistant, tamper evident, biometrically enabled, machine readable, and they serve as very reliable flashpasses.

So what is an optical card? Optical cards are extremely durable, machine readable cards with data-storage capabilities of 1.1 or 2.8 megabytes. Both visual and digital data is recorded into the reflective optical strip using a 40-millawatt semiconductor laser to brown pits into the core of the card. The data is protected beneath a 17-mil clear polycarbonate. The same stuff that we make airplane windshields out of. The data is nonvolatile and cannot be erased or fraudulently altered.

The optical strip can include visual micro- images for both covert and forensic security features, using 12,000-dots-per-inch photolithography. At time of manufacture any or all other security features and card technologies can be incorporated into the body of the card. Digital data can only be deciphered by reading the card in its matched optical memory card reader. No commercially-available reader can read from or write to a secure optical card. The data can be encrypted, but it cannot be interrogated remotely.

Because the data can be retrieved from the card itself and not from a central database, the card bearer carries his own data which he presents to an inspector under the principle of inform consent. The cardholder is always aware of when his data is read and by whom.

Let me clarify what I mean when I distinguish between nonvolatile and volatile data storage. To me volatile data storage is anything written electronically or magnetically which can be erased or destroyed imperceptibly. RFID, contact or contactless chips, mag strips are all volatile data.

Optical media technology is nonvolatile. It isn't susceptible to eavesdropping. It cannot be erased, altered, skimmed, or spooked.

I also define volatile data as something that I can deliberately disable, again, imperceptibly. I can break a chip or antenna with a hammer. I can also break it with a fingernail. You would never know just by looking at the card. Encryption and PKI are of no use if the card is disabled and will not read.

To deliberately render optical memory card unreadable without it being blatantly obvious is impossible. You have to destroy the card. If it's still got four corners, we can read it. The data and the laser engraved personalization are truly tamper resistant, tamper proof.

True biometric verification is also of key importance. DHS has deployed 1,024 biometric verification field readers for optical cards. Canada has deployed 220. They all authenticate U.S.-Mexican Border Crossing Cards and Green Cards, as well as Canadian Permanent Resident cards. There are eight million Border Crossing Cards in circulation today that have two cogent fingerprint minutia templates stored in the optical media.

A complete inspection, including card authentication, biometric verification, and display of relevant ID data can be done in less than three seconds, in the field, all from the card, not from the database. There's no reliance on database availability, no concern of network latency issues. Data security and privacy are always secured, because the cardholder controls his own data. And it cannot be read surreptitiously.

So what would I like to leave you with today?

First, data security and document security are fundamental to a reliable and successful secure ID card program.

Second, that it is necessary to design for a secure flashpass from the start. Because inevitability, some chips will not read, databases will go down, and networks will fail.

Third, the volatile data storage will always be susceptible to nefarious intent, whether it is deliberate destruction, forgery, skimming, or altering. If the integrity of the data storage cannot be trusted, security is totally compromised.

Fourth, the optical memory is deployed today and has been proven in the field to be durable, counterfeit resistant, secure data storage. It is the best ID technology available.

Lastly, a question. If you can have data privacy, data security, and document security, and RFID, why wouldn't you?

Thank you, very much.

MR. BEALES: Thank you, Mr. Alsbrooks. Are there questions from the panel?

Lance Hoffman.

MR. LANCE HOFFMAN: Well, the way you're describing it, it sounds like the greatest thing since sliced bread. So tell us in your own words what are the downsides. I've heard the upsides, what is the downsides, besides cost which I didn't hear mentioned?

MR. ALSBROOKS: Downside, I -- based on the operational scenario, the downside of this is you do have to put the card into a reader to read it. You cannot read it remotely. It can be read very quickly. I'll be glad to demonstrate that for you. You can put it into a reader. You can read the biometric template and verify a fingerprint in between two at half and three seconds.

MR. [SPEAKER]: Cost?

MR. ALSBROOKS: The cost. We charge -- for the raw cards today, we charge DHS, I believe it is $3.86. The Canadian card is a little bit more sophisticated because it has two layers of laser- receptive material. I believe those cards -- we charge the Canadians about $5.00 for those cards.

MR. BEALES: Lisa Sotto.

MS. SOTTO: I'm surprised that we haven't heard about this technology before. But it may be that that folks at DHS were thinking that it really wasn't a new and something that we were terribly interested in. But a couple of questions come to mind.

First, the data can't be destroyed no matter what you do?

MR. ALSBROOKS: You can destroy the card.

MS. SOTTO: You could destroy the card as opposed, but that's hard to do?

MR. ALSBROOKS: But the point is you cannot destroy it without it being obvious.

MS. SOTTO: So what happens if somebody loses this card that is essentially indestructible? So that's one question.

How does it link back to the individual so that you know that it's my card and not Howard's card?

And the second point that comes to mind is it's impossible to conceive of any kind of technology were some nefarious person isn't going to create a reader to be able to read these cards. I know you control these readers very tightly, it sounds like, based on your testimony. But wouldn't we need to think about the scenario of how -- of when somebody, a bad guy, creates a reader for these cards?

MR. ALSBROOKS: Okay. The cards and readers are matched sets. The media is created with an electron-beam process were you etch into a piece of photosensitive glass all of the data security features of the card. Then the card -- from that a master is created. And then the image in the optical stripe is etched at a 12,000-dots-per-inch image.

There are places in there where secure codes are written that when the card is read it has to be matched up to its -- either encoder that is used to write that card or its field reader, which is used to read it.

If there is not a match between the card and the encoder, it will not write it. If there is not a match between the card and the field reader, it will not read it.

So for a bad guy to go and replicate that system, first of all, they've got to get the system that can produce the card itself and put the right code into the correct field. Then they've got to go and create a reader/writer and get into the ROM the matched set that is going to link that. I believe there are a lot easier ways to get to this country than to do that.

I will be glad, if you want to see all of this, the manufacturing site is about 30 miles south of here in Mountain View, California. And we will be glad to go show you how all this works.

MR. BEALES: I think we have time for one more question, if it's brief. And that will be Richard Purcell.

MR. PURCELL: Quite brief. I don't know if you've heard claims that a card may not be secure, some made quite recently perhaps, but if you have heard any claims about security compromises or vulnerability to this, can you talk to those directly and in concise ways?

MR. ALSBROOKS: Well, sir, I work with the forensic document lab very closely. We've been doing this -- we first made the Green Card in 1997. We made the border -- first Border Crossing Card in the spring of '98. It has been said that these cards have been on the street longer than any other cards that have not been compromised.

I have sampled attempts at counterfeit cards that I'll be glad to show you after the -- I'm not aware that anybody has ever successfully made one of these. And you asked how you link the cards, they're linked biometrically. They are also linked with images, laser-engraved into the reflective surface that you can match. Again, I've got -- I have

sample cards here. If any of you want to see, I can bore you to death with the details. And I volunteer to do that.

MR. BEALES: On shortfall, if I could, please.

MR. PURCELL: You said earlier that a master is made of the image of -- the data image, and then that is --

MR. ALSBROOKS: It's the manufactured image in the card.

MR. PURCELL: Okay. So -- and is any residual data left behind? Once the card is manufactured, is the manufacturing process in possession of any or retains a master file or a master copy, the glass screen, whatever?

MR. ALSBROOKS: No. The photo -- it is a single piece of photosensitive glass that is created in the -- it being processed. It goes into the lab. From that a master film loop is made that transfers that data onto the individual cards. All that's done in a secure facility.

MR. PURCELL: What happens to the glass --

MR. ALSBROOKS: There is nothing -- there is nothing left over.

MR. PURCELL: What happens to the master piece of glass then?

MR. ALSBROOKS: It's preserved in the lab.

MR. PURCELL: Okay. So there -- then the identity data is preserved in a master copy?

MR. ALSBROOKS: No. This is the manufacturing process. This is not at the personalization process.

MR. PURCELL: Ah.

MR. ALSBROOKS: So the only -- what you have at that point in time is the master that creates the blank card.

MR. PURCELL: So -- and then how is the data written?

MR. ALSBROOKS: Well, today --

MR. PURCELL: The personal data.

MR. ALSBROOKS: The personal data today is written in five in -- for the DHS process, there are five integrated card production systems today. Three in Corbin, Kentucky, one in Lincoln, Nebraska, one in St. Albans, Vermont. They are secure facilities that manufacture the cards. Canada, it's made in a secure vault. The Canada cards are made in the secure vault in Ottawa.

MR. PURCELL: So once they are manufactured, is the master data preserved?

MR. ALSBROOKS: It is in a database.

MR. PURCELL: It is preserved?

MR. ALSBROOKS: Yes. It is in -- the -- yes, DHS preserves it in a database. Canada preserves it in a database.

MR. PURCELL: Right.

MR. BEALES: Thank you very much, Mr. Alsbrooks.

Our next speaker is John Gilmore, entrepreneur and civil libertarian. MR. GILMORE: Thanks. I'm going to ask my lovely assistant to pass out envelopes and stamps. Please take two stamps each. Your choice of envelope colors.

Thanks, thank you for coming to visit my town. As you're probably well aware, there are DHS guards stationed in every airport and train station, designed to keep me from going anywhere else to see you.

My talk concerns two ethics: The belief in an open society and the belief in privacy. I think these two ethics relate to each other. And I'd like to say something about how they relate to our conduct in the world.

This society was built as a free and open society. Our ancestors, our parents, our peers, ourselves, we're all making and building the society in such a way, because we believe that an open society outperforms closed societies in quality of life and liberty and in the pursuit of happiness.

But I see this free and open society being nibbled to death by ducks, by small unheralded changes. It's still legal to exist in our society without an ID, but just barely. It's still legal to exist by paying with cash, but just barely. It's still legal to associate with anyone you want, almost.

And I think conferences like ours run the risk of being co-opted. We sit here and we work hard, and we talk to people, and we build our consensus on what are relatively minor points, while we lose the larger open society.

Professor Lawrence Tribe talked at our conference about the deep distrust that we must hold for our government. We have to realize that the people who run the government can and do change. Our society and our permanent rules must assume that bad people, criminals even, will run the government at least part of the time.

This entire first part of my talk is verbatim from a talk that I gave 15 years ago at the first conference on computers, freedom and privacy. But it still seems relevant. DHS has already made the major decisions, for example, that ID is required of citizens. And all that's being talked about here is on the margins, like what to do with the resulting databases once you've collected them.

We need to go back to the fundamentals. For example, we know that the illegal NSA wiretaps have been passed to the FBI. They've almost certainly have been passed to DHS. They go into the terrorist screening database, into the watch lists. This goes squarely into your Committee's focus. Are you going to investigate it? They're trying to shut down everybody else who does. Are you going to do it?

Open societies are protected by enforceable rights. And there is no place for rights at the Department of Homeland Security. I don't mean conflicting interests or balancing tests or measurements of effectiveness. I mean inalienable rights, the kind that protects the minority from the majority. Like the right of every citizen to leave the United States, no if, ands, or buts. If you don't love it, you can leave it. Well, except DHS now says you'll need a passport or ID to exit at the Canadian border. And the government is free to withhold those at its discretion, at least according to the Supreme Court.

Or the right of every citizen to return to the United States with or without documents. It's an absolute right. If you're a citizen, you get to come here. All right. So what's this about citizens not being able to come in from Canada unless they've got documents?

Like the Fourth Amendment, now there's a dead letter. TSA argues that it has a general warrant in every airport and the courts back it up. It's a permanent dragnet with a permanent list of people to select for special maltreatment. Everyone can be searched and questioned for any purpose to any extent in TSA's infinite discretion.

I've been litigating this issue. Those people aren't free to leave if they decide they'd rather go home than travel. DHS is doing secret, detailed x-ray searches of entire cars and trucks at ferry docks. Suspicionless searches of locked trunks via Z-backscatter machines, without the owners' or passengers' knowledge or consent. Right out of the Olmsted dissent. Bus passengers arrested for failure to show ID. Subway passengers subjected to mandatory searches. Cars merely driving near airports are searched whenever DHS declares some secret reason for citizens to bend over.

The government claims that there isn't a search when only a computer scrutinizes your life history. If no human sees it, it wasn't really a search. The DHS no-fly report from this Privacy Office says they don't even check the IDs against watch lists on trains and ferries. There is no valid purpose for demanding IDs there. It's just there to track the movements of the public. Companies, states, and cameras are ordered and funded to create records about every customer and every citizen, and turn them over to DHS for storage and search. And DHS couldn't actually compel those customers or those citizens to reveal that info. But they can compel the companies and the states to create those records. And then they're free to search it, according to the Supreme Court. The Fourth Amendment, it's the zero-eth amendment.

What about the right of every person in America to move around inside the country? To use their feet, public transit, and common carriers. Free countries don't authenticate travel. Except DHS says, "You can't do that without your documents." Oh, except if you're on a secret blacklist, like hundreds of thousands of other people, then you can't travel at all, even with your documents.

Talk to Robert Gray, the Long Island pilot who sued TSA for no-fly-listing him without cause. That case is still pending.

What about the right every person to be able to read and know what the laws are? The published regulations from the General Services Administration about federal buildings say they're open to the public during business hours. There's no mention of IDs. But the guards who work for DHS enforce the secret law.

There is no published regulation or law that requires ID on trains, buses, ferries, or planes. Yet 99 percent of passengers have to show an ID to get onboard. The judges in the Gilmore versus Gonzales case announced in their opinion that TSA doesn't actually require ID to fly. So what that means is the signs in the airport that TSA put up are all lies. The airline employees are ordered to lie to the passengers that ID is a requirement. Or maybe they merely have no idea what the law that they're enforcing really says, since it's a secret law.

Well, the citizens don't know what it says either, so they can hardly contest it. When this news came out of the court, and reporters, some of whom are in this room, called up TSA and said, "So what's with the signs in airports, why do they lie?" The TSA spokesman said off the record, "Oh, they're lying to passengers so that TSA will have to do fewer physical searches."

So let's get this straight. TSA has its own secret rule somewhere. Apparently it requires anonymous passengers to undergo an unusual physical search. But because that would be too big a burden if applied to a normal population of Americans, some of whom would and some of whom wouldn't have an ID, TSA lied so that citizens will bring and show their IDs, even though the citizen didn't actually need it and TSA didn't actually need to see it.

Instead of lying, TSA could change their rule. Personally I think that officials who entrap Americans into voluntarily giving up their rights by lying to the public about what the law says is a far worse tragedy then crashing an airliner. Destroying the rule of law for their own bureaucratic convenience is not a small matter. And of course now that ID is demanded all over, we need to be sure these IDs have a proper data shadow, dogging every citizen's every move.

The ID demands are used to bootstrap the cradle-to-grave national ID system -- forgive me -- I mean the Real ID distributed database.

The mandatory SSN in that database then ties the citizen, who uses his state ID, to all the other databases. Every cop is trained to demand and record ID as step two of every encounter with a citizen. And DHS plans to automatically start logging every contact with the government forever, using RFIDs.

DHS fills public spaces with its own cameras while harassing any citizen who uses their own cameras in the same public spaces.

The homeland is not secure with DHS in it. It's the neutron bomb of security. The buildings and the infrastructure are all undamaged. But all the rights are dead. It leaves the country ready for easy takeover, foreign or domestic. Who will protect the homeland from corrupt officials, from incompetent or mean-spirited public servants, from internments, from McCarthyism, from the Nixons, the J. Edgars, from a secret coups, secret laws and secret prisons? The citizens will protect the country from this?

DHS is training them all to live in a police state. DHS is building the mechanisms of detailed social control. DHS arguably violates 70 percent of the Bill of Rights on every day.

Now I looked at the minutes from the last meeting where you had lots of DHS executives. They could've testified to your Committee along the lines of, 'If we could act like Mussolini we could make the trains run on time,' right, or 'Make the homeland secure,' or whatever. But that's not how they think. They don't bother. They say, "Our job is to make the trains run on time." They already assume they have the powers of Mussolini.

So Privacy Committee Members, I charge you: DHS is prosecuting a war against both freedom and privacy. Expose it, publicize it, stop it. DHS and TSA lie to the public. Their pretty No-Fly Report lies on page 1, saying airlines must collect personal information from everyone who travels by air. The court put the lie to that. It's not a requirement.

Find out some of the real rules. Here's how. I brought you envelopes and stamps for each of you. Mail all of your government-issued photo IDs to yourself at home. Put them in the envelope and mail them home. Okay? Become an unperson, an undocumented person, an illegal citizen. Then fly home from this meeting without an ID.

Tell DHS you don't have it or that you decline to show it. You'll find out what the real rules are that enforced against the real citizen who care about having real privacy. Are you afraid to? You have very good reason.

MR. BEALES: David, I think we just have time for one brief question.

MR. DAVID HOFFMAN: I won't take you up on your offer, because I live in Munich, Germany and the German government would be very displeased with me if I tried to enter their country, I think, by doing that.

But the question I have for you is if you were allowed to travel without documents but were subjected to a higher level of searching because you were traveling without documentation, is that acceptable to you under your Fourth Amendment analysis? And if so, to what degree?

MR. GILMORE: There are two issues there. The first is what the real rules are and the second is how do I feel about them. If the real rules were as the court stated, that people are free to either opt for a more intense physical search or showing an ID, at least people who don't want to show an ID, who don't want to build a data shadow, could get around in their own country. But those aren't the actual rules. Even in the facts of my own court case, I was denied boarding on an airline, which never offered me a physical search. And on the way back from Washington last month Ed Hasbrouck tried flying without ID and was almost arrested.

As to whether I feel that person who wishes to exercise their fundamental right not to incriminate theirselves, not to agree to a search, should result in a heightened level of suspicion, no, I don't think that a person who wishes to be anonymous should get any more intense search than anybody else who goes through an airplane. Right, if they're carrying weapons or explosives, find them. If they're not, don't hassle them.

MR. BEALES: Thank you, Mr. Gilmore.

Our next speaker will be Daniel Mullen, from AIM Global.

MR. MULLEN: Thank you, Mr. Chairman. I appreciate the Committee taking some time at the end of the day. AIM Global is pleased to have the opportunity to speak to this Committee in response to the Draft Report prepared by the Department of Homeland Security Merging Applications and Technology Subcommittee. And we appreciate the opportunity to provide those comments.

A little background. For more than three decades AIM Global and our members have been the leaders in developing automatic identification data collection technologies, standards, and best practice around the world.

AIM Global is an ANC-accredited, ISO- recognized, international not-for-profit trade association, representing providers of technologies, such as radio-frequency identification, barcode, mobile computing, magnetic stripe, and biometrics. These technologies are key components in providing convenience, productivity, and security benefits we take for granted everyday.

In reviewing the Draft Report we can agree with many of the recommendations found on pages 12 through 14 of the Report regarding best practices to be employed when using RFID.

As consumers first and industry members second, AIM Global supports strong policy and protections for personal privacy. For several years our RFID Experts Group, or REG, has been hard at work crafting best practices for RFID implementation guidance related to privacy, security, recycling, and many other areas.

AIM Global was the first to develop a standard global-unique emblem to identify the presence of an RFID tag on a label or inside an object. This unique design has been welcomed by public interest groups.

As applications for RFID technology have expanded, RFID providers have responded with unparalleled innovation to deliver the needed technology tools to aid in effective solutions with appropriate levels of security and privacy based on the given application. AIM Global members are diligently working to develop technology-based solutions to the issues of privacy and security.

In light of our position as an association representing experts in automatic identification technology and a responsible participant in the public policy debate, we must disagree with the Report's conclusion that RFID be disfavored for identification management.

The benefits of using RFID in identity documents are compelling, and recommending that DHS not use it would deprive the Department of a powerful tool with which to meet its critical mission objectives.

While there were a range of unsupported summary statements disparaging RFID technology in the Report and a failure to consider the ways in which RFID technologies are already being used to enhance security at U.S. borders and recent technical advances that help ensure privacy, considering the time limitations today I want to focus my comments in three areas: AIM Global's perspective on security and privacy, RFID as a family of technologies, and the positive applications of RFID today.

The RFID family -- this is an essential point -- the Draft Report addresses some commonly- raised security questions related to the use of RFID. Unfortunately, a large source of misunderstanding surrounding RFID has been created by the temptation to simply refer to all RFID generically. It is absolutely essential to recognize that RFID is not a monolithic technology. Rather, it's a family of similar but not identical systems, each with its own capabilities and limitations.

For instance, there are four primary frequency bands: LF, or low-frequency; HF, or high- frequency; UHF, ultra high frequency; and microwave. These frequency bands are for RFID technology and several possible types of tags within each frequency band exists.

Furthermore, RFID tags can be designed with different amounts of memory or ancillary features that support a given application.

While we do not have time today to go into detail about the different types of RFID systems, it is really important to realize that each member of the RFID family has a different set of capabilities and limitations. Different data collection applications require different levels of security to ensure privacy.

Attempting to discuss RFID in a one-size- fits-all approach to the privacy and security would instead result in a one-size-fits-none solution that could deprive consumers and businesses of existing and future benefits of this technology. Instead, AIM implores you to first understand completely the capabilities and limitations of each member of the RFID family. Then you will be better able to evaluate the processes that might be aided by automatic data collection and the specific types of RFID that could provide these benefits.

It's important to emphasize that the evaluation must be done at a systems level, considering the type of data to be encoded, the intended read points, built-in and external security measures. It's only with this system's view that a true picture of which technology or technologies can best fulfill the application.

RFID designs used in automatic identification applications can include strong cryptographic protections against unauthorized access to data on a card and unprotected transfer of data to and from the card. Systems design can also employ chip level techniques which preclude tampering or modification of data on the chip and systems that detect cloning of the data on a chip itself. One of the fundamental benefits of RFID technology and human identification applications is that it can be combined with the strongest most current cryptographic methods and secure chip designs without compromising the basic performance benefits of the contactless technology.

A little bit about AIM Global's perspective on privacy and security. In discussing applications of RFID, AIM Global believes that a best practices, policies, and procedures should be put in place to ensure appropriate privacy. Within the past year AIM Global has issued our perspective on RFID privacy and security for consumer-oriented applications.

AIM Global believes that the use of RFID for human identification programs can be a powerful tool for both the U.S. government and U.S. citizens. AIM Global would recommend that an agency intending to issue remotely-readable government-issued identification credentials should ensure that: The issuers incorporate tamper-resistant features to prevent duplication and forgery; the issuers require authentication between a card and reader; and in the case of credentials containing personally-identifiable information, such as a person's name, date of birth, and/or home address, the issuer

employ secure protections for data stored in the credential as well as data transmissions between the card and reader.

Finally, a little bit about applications of RFID. RFID systems are currently in place within the U.S. government that help provide security while facilitating the efficient transport of goods and people at U.S. borders. Passive UHF RFID has been in use in U.S. borders for nearly ten years in several related trusted-traveler programs, such as NEXUS, SENTRI, and FAST. To date there have been no reports of which we are aware that indicate abuse or monitoring of the nearly 900,000 users of this program.

Passive HF RFID has been selected for use in passports by IKO and dozens of nations as the standard for new passports containing biometric authentication. Proposed systems can provide further benefits to Homeland Security, including: Document authentication, such as the US-VISIT Passport and pilot licenses; expedited recordkeeping of border crossings for trusted travelers and a guest workers; biometric information to enhance comparison or validation of electronic documents, electronic records, and the individual; container identification and security seals to enhance C-TPAT, safe and secure trade lanes, and other U.S. government initiatives; helping to ensure the security and integrity of the pharmaceutical and food supply chains by enabling current FDA and USDA initiatives for product authentication, anticounterfeiting, product diversion.

If anybody watched "Dateline NBC" this past Sunday, they featured a story about the pharmaceutical arena. And we believe there's a strong case for RFID use in this area.

Product, pedigree, tampering prevention, livestock identification and tracking, are also areas that it can be used and is used.

Helping to increase the efficiency, accuracy and the velocity of the supply chain, resulting in faster retail response to customer needs, greater selection, availability, and lower prices.

While it's acknowledged that RFID will provide significant benefits to citizens' safety in programs such as C-TPAT, safe and secure trade lanes, as well as pharmaceutical and food-supply tracking, AIM Global's position is that DHS should not limit the technology's potential benefits to providing security based on some unsubstantiated and technically-feasible concerns about privacy.

Finally, AIM Global supports the appropriate and secure use of automatic identification technology by providing unbiased professional information on the technologies and their uses. We appreciate the Department's commitment to protecting individual privacy. We share in that commitment.

We also appreciate the Department's dedication to the core mission of protecting the American people from terrorist attacks and other threats. We trust the Department

will continue to deploy information technology systems that will allow it to achieve both goals.

AIM Global would be happy to work with Members of the Advisory Committee to rewrite this Report that better reflects an understanding of RFID technology. AIM Global, our RFID Experts Group, and our members stand ready to provide impartial expert advice on RFID and other automatic identification subjects.

Thank you. And I'd be happy to take any questions if there are any.

MR. BEALES: Thank you, Mr. Mullen. I think we have time for one question. Mr. Sabo.

MR. SABO: Just one quick question. Does AIM Global have a set of privacy white papers or guidelines on addressing privacy in RFID technology irrespective of the band or the frequency?

MR. MULLEN: We particularly have an RFID -- our perspective on RFID and privacy and security as it relates to the consumer arena, because that has been such a hot topic within the RFID. But we are currently looking at other areas, as well.

MR. SABO: I guess I'm thinking in terms of human identification, which was the focus of the Subcommittee Draft. I mean do you have informed guidelines on that --

MR. MULLEN: No, not at this time. Not at this time, no.

MR. BEALES: Any other questions? Joe.

MR. ALHADEFF: And I guess this is kind of a similar question as to whether these resources exist or not. Part of the choices that DHS faces with the deployment of any technology is choosing among a range of technologies. And I was wondering if your association or group has put together any comparative analysis of security benefits, you know, risks associated, et cetera, et cetera, between the concept of contactless versus contact, different types of security, different types of mechanisms, or has it focused solely within the RFID space or the sensor- based space? MR. MULLEN: Well, we represent all ranges of automatic identification technologies. And we would be happy to work with the Committee to provide that sort of information. Absolutely.

Thank you.

MR. BEALES: Thank you, very much.

Our final speaker on this public panel will be Neville Pattinson from the Smart Card Alliance.

MR. PATTINSON: Good afternoon, Chairman and distinguished Committee Members and Acting Chief Privacy Officer. It's a privilege to be able to speak to you this afternoon.

I represent the Smart Card Alliance. This afternoon, I can wear several hats. But I shall be the Smart Card Alliance. I also -- I'm on the Board of the International Biometrics Industry Association. And I also work for a smart card company.

The Smart Card Alliance, who I do represent this afternoon, is a not-for-profit multi-industry association working to stimulate the understanding, adoption, use, and widespread application of smart card technology. So this is your education session this afternoon. And that's what I'll be mainly doing.

I'm not going to read a prepared speech. I'm going to go through few points, and hopefully there are some questions and we can continue the education of the Committee.

First of all, regarding the RFID for Human Tracking Draft Report, I've submitted comments and so has the Smart Card Alliance. First of all, we certainly don't think this is appropriate use to track humans. RFID or any technology shouldn't be used to track humans. It should be used for identification purposes. And I think what we need to look at is authentication of the individual and to verify their identity when we have devices that have been issued to the individuals.

Clearly, there's still an enrollment aspect for them to get into the system. And there's also a vetting process before the enrollment. But once the vetting and enrollment's been done we now need to look at is this person who we've got in front of us the rightful owner of this document. Can we tie them together. And can we therefore establish and then verify their identity is indeed as it was given to them when they were issued that document.

So moving back to RFID and to reflect comments that you've before, RFID is not one technology. It's a range of technologies. And very specifically I'd like to segment them. RFID, in my terms, coming from the smart card community, is a technology that's traditionally been used for tracking pallets, cases, and products. And that's been its strength. It's very good for the commercial tracking of goods and services through the supply train.

It is attempting to present itself for human-identification purposes, which I fear it is woefully inadequate. Smart card technology, however, that we've been making for over 25 years, and is in use in billions of instances around the world, is a technology based on silicon chips, as RFID is. But it's based on very sound and secure silicon chip construction practices, security mechanisms. Typically over 200 security countermeasures and features exist in smart card technologies, which allow a great deal of confidence in that technology to be able to perform its purposes.

In the last five or six years we've seen the adoption of smart card technology into identity applications. The biggest one being right here in the United States. And I'm proud

to be having been part of that program in the supply of the Common Access Card to the Department of Defense.

So smart card technology is proven. It is secure and it is a very appropriate technology to use in identity applications. It uses government-approved encryption algorithms, according to the FIPS 140-2 standards and is all built on open standards. There's nothing proprietary about smart cards. Any company can produce one according to the open standards, unlike optical technology, which you heard from earlier, which is a proprietary technology available from one company.

So RFID, let's use the term "RFID" for a technology that's for tracking items. And let's use "contactless smart card technology" which is used for providing identity authentication and identity verification of individuals.

We've heard the Epassport mentioned several times today, and even the State Department calls it RFID. But perhaps I'm being pedantic, but it's not RFID. The Epassport is based on smart card technology and, specifically, contactless smart card technology.

The privacy issues that blew up a few years ago over the Epassport Program, I've been personally involved with those., trying to bring the appropriate level of security to bear in order to ensure the privacy of the citizen around the country and around the world, as they carry their electronic passport.

The State Department has now adopted a very thorough and comprehensive set of privacy practices and security mechanisms within the electronic passport to make it a highly-trusted and very successful document now. IKO still states -- I mean making recommendations rather than mandatory use. The State Department here has gone further, and I applaud them for that. And I think we should be proud that the Epassport now is in a state that will preserve the citizen's privacy.

The Faraday cage, you heard before. Why don't we just pop cards and things into Faraday cages, and passports. Well, yes, the passport does have a Faraday cage in the front cover. As it closed, it won't be read if it's open. It can be read, but when we say can be read, it can't even be detected. When it's opened, it still can't actually be read until you've swiped the physical page and obtain codes in order to open up the chip and then provide a secure channel to the chip.

Faraday cages are a subject of debate. And I think we'll find that that is really where technology has failed to meet the policy required of implementation of the application. We should be able to identify correct practices with technology to support identity applications that do not require the use of shields or Faraday cages in normal applications.

We can use, as we have in the electronic passport and other identification documents, random identify numbers that come out of the devices initially. They can then perform a cryptographic mutual exchange with the reading equipment to verify that they are both known and trusted to each other. And then they can perform encrypted communications between the two devices. These are sound security practices. They don't need Faraday cages.

We've heard today about the Western Hemisphere Travel Initiative Project, which again appears to be moving along in the direction of taking a UHF RFID to work over 30 feet of distance. This is an insecure technology. It's the Generation 2 technology. Its security is based on a 32-bit password to gather information on the device. That is not government-gate encryption. It's static. It's subject to many different attacks and still is woefully inadequate for the needs of this application.

Contactless smart cards are much more appropriate. We've demonstrated this to the State Department and to the DHS US-VISIT team. The comment this morning from Mr. Yonkers about not wishing to wind down the window to put the cards on the reader I think is very peculiar, because you're going to have to wind down the window to talk to the immigration officer, anyway. So I'm very puzzled as to why that's seems to be an issue.

Our technology, a contactless technology of smart cards, works over a few inches. It can't be detected over 30 feet. You can't be tracked going down the road or by somebody in a car going down the road. This stuff will only work over literally inches and is therefore secure, which is why the electronic passport has adopted that technology as well as now the government PIV credential in response to HSPD-12. That is using contactless smart card technology as well.

The Transportation Workers Identification Credential for Maritime is on the move again. And that would appear to be using the same principles of secure smart card technology, rather than any RFID technology.

So putting a chip in a document actually does several things. First of all, it increases exponentially the difficulty of frauding the document. Instead of just being able to have to reprint it or make a clone, you now have to have a chip. Not just a chip, you have to have an operating system. Not just the operating system, you have to have an application. Not just the application, you have to have the data. Not just the data, you have to have the cryptographic keys. It puts many levels of additional security into the identity document.

You can use it in conjunction with biometrics. The smart card technology is able to match fingerprint, facial information inside the chip, inside the card. We don't need to match outside the card. It could be done by the secure computing resources inside the smart card technology.

You can securely communicate its information externally to the card. It can do that encrypted. And it can do that in a privacy-enhancing manner, making sure that only the information that needs to be transmitted is transmitted. Not all of the information. It can be very selective. And it is always very protective of the information it contains.

We heard of Real ID this afternoon as well. This is an opportunity to see where smart card technology with the combination of biometrics in that identity card is really what the Real ID should have been about and I think it can still be about. We are trying to identify a person. The way we identify a person is with identifiers, a smart card, a biometric. Put the two together, you've got two factors of authentication. Add a PIN code, if you want, for a third level of authentication and use a control for releasing information.

We see therefore Real ID is an opportunity to really make sure that you do know who you have standing in front of you, not just the document that claims somebody is who they are and it's up to you, standing there, to try and work out if they do match. You can get the smart card to help you do that.

So in summary, I really see the response. And your direction, I would encourage certainly to define the privacy and security policy with respect to citizen identity applications, independent of technology. At the moment the Report is about RFID for tracking and identification. I think we need to rethink that and look at how to define the security and privacy policy with respect to citizen's identity, without specifically mentioning technologies.

We should look at best practices, in privacy PIAs and so on, and anything else to do with the technology, as biometrics, whatever that may be used, how that data should be used and secured and so on.

We should also select then technology, once we've done that, based on standards, not proprietary technologies, things that are open and available and commercially competitive. And we then should have obviously review-and-check-and-audit procedures in place to make sure that it is working and meeting the needs.

So then I conclude my comments. And I thank you very much for the opportunity to speak. And I certainly make myself available for comments, for questions.

MR. BEALES: I think we have time for when question. John Sabo.

MR. SABO: Just a quick question. From your perspective, what -- given as you described the process, you got to swipe the contactless ID in order to do an authentication of the card or whatever the -- to unlock the data and allow it to transmit or to be -- or to have it --

MR. PATTINSON: For the E passport, that's --

MR. SABO: Yeah, the E passport. What is the -- there's a big discussion around contactless versus contact, irrespective of distance. What is the advantage of going contactless if you've already got to place, in effect, this card into a reader of some type?

MR. PATTINSON: First of all, the passport is an open-security environment. You have data, personal identity information on the passport issued by various countries around the world. And what we're doing is restricting the access to that information so that only after you've opened the passport, swiped it, got the password, opened up the chip, done the secured channel, got the payload out, encrypted, and decrypted it, then you've got the information in front of you electronically, digitally signed, according to the country of origin. You can then verify that data.

You can look at the printed page. They should match. You can look at the person standing in front of you. They should match. You don't have any databases you're going online to. This is an offline database.

MR. SABO: Right. But I guess my question is why contact versus contactless. In other words, why can't you just --

MR. PATTINSON: I'm coming there.

MR. SABO: Right. Okay.

MR. PATTINSON: So on the basis of why contact and why contactless. Contact is traditionally a very successful technology. It has been used in millions of applications. In transportation and in transit and in high-volume passage, it is much more efficient to use contactless technology. Don't have to plug it into readers that may wear out, may be subject to dirt, and so on.

Contactless technology is also faster in its communication. We can get to speeds of 848 bits per second, whereas the contact is a fraction of that speed. So we can get a much faster communication speeds and deliver photograph and payload, and very much more efficiently. You also don't have form-fact issues, if the passport gets bent or misshapen, it won't fit in the reader. You can just lay it on the reader. It'll work very reliably.

Does that answer your question, sir?

Thank you.

MR. BEALES: All right. Thank you, Mr. Pattinson.

MR. PATTINSON: Thank you.

MR. BEALES: That concludes the public panel that was selected in response to the Federal Register Notice.

We now move to a period of public comment in which speakers who have signed up will have three minutes to address the panel. We will not have time for questions. And our first speaker will be Edward Hasbrouck.

PUBLIC COMMENTS

MR. HASBROUCK: My name is Edward Hasbrouck. And unlike the Members of this Committee and of today's panels, my background and domain expertise are in the travel industry, travel technology, and advocacy for travelers.

There are two sorts of expectations of privacy: Those that people actually have and those that the law presumes us to have. But by either measure expectations of privacy in public spaces are not just about our right to be in those places but about our right to move through them. To assemble is not just to be together but to come together.

When we assembled here today from throughout the country, by various means of travel, our journeys were acts of assembly, directly protected by the First Amendment. Freedom to assemble is an inalienable human right, not a privilege to which citizens need to prove our entitlement. We expect that our privacy includes the right to move through public places on public rights-of-way and by common carriers without let or in hindrance and without demands for government-mandated credentials.

Orders restricting the right to travel should be issued only on the basis of a judicial finding subject to adversarial challenge and due process. That's what's required thousands of times every day when someone in imminent danger of domestic violence seeks an order restraining the right to use the public right-of-way adjacent to their home by someone they believe poses them a danger. No lesser standard should be applied in the case of people alleged to pose a danger in other places.

We also expect that while our movements may be observed the government will not keep a file on us without due cause. But given the ease of data mining and the ease of government access to commercial data, there is no longer a meaningful distinction between event logging and the construction of personal dossiers, or between logs held by private entities and those assessable to the government. To allow unregulated commercial logging of events, especially those identifiable with a time, a location, and an individual of which travel reservations are the canonical example, is in effect to allow the operation of a continuous submit of universal, suspicionless surveillance in flagrant violation of our expectations of privacy.

Perhaps the most egregious violation of travelers' privacy comes when we are compelled by the government to provide information to commercial entities as a condition of the exercise of our right to assemble by common carrier without any constrain whatsoever on the ability of those commercial entities to retain, use, or sell that data.

I urge this Committee to recognize the centrality of travel to the privacy impact of DHS activities and to focus your work on the specific issues of: The right to assemble; the mandate for travel credentials; the basis and procedures for government orders restricting travel by specific individuals; the retention and use of reservation and travel logs; government mandates for the provision of information to nongovernmental entities, such as airlines; and the need for a federal privacy law applicable to commercial travel data.

I look forward to assisting the Committee in these endeavors. Thank you.

MR. BEALES: Thank you very much.

Our next speaker will be Nicole Ozer -- Nicole. Okay, then we'll move to Louis Parks.

MR. PARKS: I guess the first thing is I've got somebody's watch. Thank you for these few quick moments. My name is Louis Parks and I'm with a company called Secure RF. And we've developed security protocols that actually fit on passive RFID tags. And in fact I was very happy to hear Steve Yonkers, who has been supplied with some of our documentation, reference some of our work earlier today.

I guess in the few minutes I have I just wanted to say that, you know, the assumption I'm sitting here, as many people are, is RFID the train has left the station, and I guess the issues are still at the track at the other end. So just the little bit of input as we're doing that.

You know we keep talking about a lot of different technologies and obviously that hasn't been resolved. And I'm saving a lot of my time by having the Smart Card Alliance educate us on what smart cards are. But passive RFID and smart cards are totally different technologies. And, yes, there are security protocols that exist on smart cards, and I can't speak to laser cards, but it's an area called symmetric security. And there are papers that have been published.

There is one actually that we reference in one of our papers from Cambridge University that shows a 150-foot read range on the same technology they're using. So the idea that because it's a short read range you're better protected may or may not be the case. So I'm not sure.

But I guess, you know, there are solutions that exist. We actually supplied a paper to Homeland -- to the Smart Alliance group on how to put authentication and encryption security on Gen 2 tags, some of which was just referred to in the discussions that were here. And there are some real benefits, particularly when you stay in the asymmetric or public key arena. The ability to turn on and off cards, the ability to revoke credentials, which may be something of interest once you've issued these cards.

There's a lot of flexibility and I think a lot of extension of the technologies that have been discussed that come to bear over and above the paper that was published or about various individual data points. So it's really a function of setting up the menu of functionality; 96 bits, for example, is simply the standard implied by EPC Global. You can go bigger, you can go smaller. There are security technologies that can go on, and I think that the Committee continuing to create open channels for some of us to provide additional information will probably lead to a great solution. Thank you.

MR. BEALES: Thank you very much.

Our next speaker will be Kevin Mahaffey.

MR. MAHAFFEY: Thank you. My name is Kevin Mahaffey and I am a security researcher with Flexilis. First I would like to commend the Committee on the emerging applications and technology. Their Draft RFID Report document and its framework and best practices has very many valuable insights into RFID security. And as many new RFID pilots are proposed, it will allow them to avoid common security and privacy pitfalls.

I would also like to bring to attention to the Committee that read range should not be used as a security measure in RFID technology. For example, in the United States passports initially no security was implemented because read range was assumed to be limited to only a few centimeters.

Later security was implemented because they demonstrated a 10- to 15-centimeter read range, and it was assumed that you can't just have no security when that kind of read range is in consideration.

In actuality the theoretical maximum on that technology is up to three and a half meters of read range. Such nominal read ranges assume a lot about the implementation and the current condition of the environment that are being tested and rely on many technical details to determine.

Also with UHF technology, last August by using modified equipment available commercially I was able to demonstrate a 69-foot read range of UHF tags. This could be extended much further with additional equipment.

Read range is a very important consideration for this Committee because RFID tags cannot be allowed to be surreptiously read or cloned for both security and privacy reasons that need not be stated. These surreptitious reading and cloning can be prevented with proper cryptography and physical counter measures. However, it's very important to realize that encryption is not just a check box that ensures security.

All of these security measures need to be evaluated very comprehensively in the context of their real world systems. For example, protocol identifiers outside of encryption

can be used to uniquely identify a smart card or contactless chip, or whatever we want to call them. We all know what they are. And with this unique identifier you can serve to infringe privacy or security, or whatever you wish to do for it.

And with respect to the US-VISIT Program, this pilot certainly has problems that have been identified by the US-VISIT program themselves and others. However, it's not final. It's simply a pilot. And I like that they're approaching an iterative development process and are opening the table for security vulnerabilities so that outside experts can take a look at the system and perfect it before it actually gets deployed. And they essentially are walking, not running to embrace this new technology.

We can make RFID secure, but we need to pay careful attention to the implementation details in the context of the real world use.

And thank you very much for your time.

MR. BEALES: Thank you.

Our next speaker will be Dazza Greenwood.

MR. GREENWOOD: Dan.

MR. BEALES: Dan.

MR. GREENWOOD: Yes.

MR. BEALES: Hello. Okay. Thank you. I'm sorry.

MR. GREENWOOD: Not at all. No, don't be sorry. You've -- you are assisting me in making some comments now.

My name, my given name and the name that appears on my license issued by the State of Massachusetts is Daniel Greenwood. And, as it happens, my nickname that I'm commonly known by, including consulting circles and friends and family, is Dazza. It's a name I picked up when I was living in Australia.

And it just raises the question in my mind -- oh, I'm sorry, just by way of introduction, I'm a lecturer at MIT, where I've been since '97 and I'm at the Media Lab, run a research institute there called the Ecommerce Architecture Program, looking at the intersection of law and public policy. Before that I was a state government lawyer doing technology, privacy, and so forth. Anyway, I think what that -- and my area of expertise is authentication and identity.

I think what that demonstrates in part is the question of your names and identity, and what they mean, and where they come from, and who owns them. One of the things that we're doing at MIT's Ecommerce Architecture Program in the Media Lab is starting what we're calling an identity autonomy project, where we're looking at sources of identity for free peoples.

Interestingly, the initial research that we've done, looking at common law and other sources of jurisprudence and political philosophy in literal cases in the U.S. and some statutes, is it shows this topic has been discussed many, many times in the past. And the last time there was a lot of case law on it was when the Thirteenth Amendment was being considered, shortly after slavery.

Slaves, who gives the names to slaves and to serfs, and so forth. What's the owners. Owners name property. So the ownership of a name -- I'm sorry -- the power to name, some say, is the power to control. And so one of the things we're looking at is who owns the names in some of these new national identity systems that are beginning to emerge.

It seemed to me when I was a state government lawyer that there was some subtle creep as we created larger and larger data systems where we, as the DMV of California Director that was just here, just to determine things like how many characters were to be, what characters are permitted, when can you change your name, when is it terminated, these are all types of indicia of control. Figuring out what criteria and who approves or denies naming rights, are part of ownership and control of naming. Naming is of course only part of identity, but it's an important part.

So, at any rate, we're taking a look at some of the underlying American jurisprudence and philosophy of people who are free, name themselves, and looking at how that extrapolates to technical architectures and policy architectures. There will be a white paper coming out on that soon.

I wanted to make the Committee aware of a couple of things briefly that we're doing at MIT that are relevant to your work. The first is an initiative with Real ID, making the good offices of MIT available as a neutral public forum for industry, government, privacy groups, and others to come together to continue an important and, I'd say, under-developed public dialogue on this very significant new legislation.

We've had one large conference and an online conference already with the ACLU, Homeland Security, and vendors and others. We'll be having another one in October. And the proceedings were given to your Policy Officer Stew Baker. But we'll also, I'd be happy, to make it available to you.

And also we have an RFID and privacy initiative, and you can find out more about that at RFIDprivacy.mit.edu. It's primarily geared at this point to consumer education, education for legislators.

And, finally, I just wanted to let you know that in my other capacity, in the consulting capacity, what has my interest the last couple of years is a potentially very powerful enabling technology for balancing privacy as well as the security and reliability interests that are necessary in the emerging identity infrastructures that we're building

out, is this Federated Identity Management technologies that the gentleman from Sun and others have foreshadowed.

Having written the rules for various federal agencies that are using these systems, such as GSA's Eauthentication Initiative and other consortia estates that are sharing identity information and trying to devolve -- I'm sorry, I'm getting email -- trying to devolve autonomy down to individual levels or lower levels, I have found that these are powerful architectures.

And I would like to suggest to the Committee that as you look at DHS' purview in these systems, especially the Real ID purview, that you consider these kinds of architectures and approaches with consortia, perhaps, of states who can develop the rules for the network system so that it becomes something that can raise that floor for privacy and due process higher than what we saw in the statute or what we can, I think, expect to see in the implementing regulation for Real ID.

So thank you for your time.

MR. BEALES: Thank you.

Our final speaker today will be Carol Henton.

MS. HENTON: Thank you, Mr. Chairman. I'm Carol Henton. I'm the Vice President of the Western Region for the Information Technology Association of America. And I appreciate the opportunity to make a very brief comment today about the Draft Report on the use of RFID for human identification.

ITAA provides global public policy, business networking, and national leadership to promote the rapid and continued growth of the IT industry. We have about 350 corporate members throughout the United States.

While we agree with the Draft Report's assertion that the steps should be taken to protect personal information, we disagree with the conclusion that RFID is inappropriate for use in all individual identification programs. Rather, we feel that the decision on what technology should be used should be based on the business case or on the requirements of the particular agency's needs.

We suspect that many of the misunderstandings highlighted in the Report stem from the lack of sufficient industry representation on the Subcommittee. (Laughter.)

MS. HENTON: We hope that any report in its final version should be based on strong factual record and input from all parties. A review of the few examples of such assertion should help the Committee identify areas where the Report's analysis could be strengthened, which in turn may affect the Report's final conclusions.

We appreciate the sincerity and good intentions of the drafters of the Draft Report. And we would be happy to work with the Members of the Advisory Committee to clear up any misunderstandings about this technology and correct some of the weaknesses of the Draft Report.

So, in closing, we appreciate the Department's commitment to protecting individual privacy and we certainly share that commitment as evidenced by the IT industry's ongoing protections for privacy and security. And many of these protects, of course, were highlighted in the Advisory Committee's Draft Report.

Thank you very much.

MR. BEALES: Thank you.

I want to -- Jim.

MR. HARPER: Sorry to make noise, but I've read the Gilmore case and I'm a California lawyer. And twice it says that the law is that you have an option between showing ID or getting secondary screening at the airport. So John has effectively posed a question to me whether I believe what I read and my legal education or whether I believe the signs at the airport.

So I appreciate his insistence on rights, his firm insistence on his rights and ours. I also appreciate his sense of whimsy and playfulness, as reflected in the brightly-colored envelopes that he handed out to us and the stamps. They're all quite brightly colored, reflecting each state of the Union. A wonderful, patriotic message.

So I've put my driver's license, the one piece of government-issued ID that I carry, into my envelope. I've put the stamp on it. (Applause.)

MR. HARPER: Thank you. It's not that good yet.

We have influence because of public discussion, and I'd like to offer to give this envelope to any reporter who will meet me at San Francisco Airport tomorrow. I fly at 8:30, so maybe at six o'clock. And I'll give you the envelope and go on my way. So the challenge is issued to any reporter who wants to come down to the airport and watch the fun.

And I'd like to challenge my colleagues to also believe in the law, because the law is now known thanks to the Ninth Circuit decision, and we should really question whether we stand for the law or whether we want to just sort of mosey along.

Thank you.

MR. BEALES: I want to thank all the Members of the Committee for very hard work over the last couple of days. I want to wish Jim the best and I hope to see you again. (Laughter.)

MR. BEALES: Thank you all, and the Committee stands adjourned.

(The meeting was adjourned at 5:30 o'clock p.m.)